

BTI 7253: Network Security

Christian Grothoff

BFH

1.3.2019

“The means of defense against foreign danger historically have become the instruments of tyranny at home.” –James Madison

Computer Security Dictionary

Hacking

Software vulnerabilities

Social Engineering

Skynet

Ethical case studies

Conclusion

Part I: Motivation

Commercial tools: The crime fighting genie!

<http://www.stealthgenie.com/> (6'2013)

Ethics

Ethics involves systematizing and recommending concepts of right and wrong conduct.

Meta-ethics What is the nature of moral judgements (universal, relative, nihilist)?
Why should one be moral?

Normative ethics How can we answer ethical questions systematically?

Applied ethics Provides answers to specific issues.

Normative ethics: Virtue ethics

Virtue ethics, advocated by Aristotle with some aspects being supported by Saint Thomas Aquinas, focuses on the inherent character of a person rather than on specific actions.

- ▶ Morality comes as a result of intrinsic virtues.
- ▶ Plato's Republic describes the Four Cardinal Virtues: wisdom, justice, fortitude, and temperance
- ▶ Different people, cultures and societies often have different opinions on what constitutes a virtue.
- ▶ Debate on what specific virtues are morally praiseworthy continues.

Virtues

A *virtue* is a trait or quality that is deemed to be morally good and thus is valued as a foundation of principle and good moral being.

Examples:

Clementia (mercy) mildness and gentleness, and the ability to set aside previous transgressions

Disciplina (discipline) upholding the duties of citizenship

Frugalitas (frugality) economy and simplicity in lifestyle, without being miserly

Industria (industriousness) hard work

Veritas (truthfulness) honesty in dealing with others

Benjamin Franklin

Temperance Eat not to Dullness. Drink not to Elevation.

Silence Speak not but what may benefit others or yourself. Avoid trifling Conversation.

Order Let all your Things have their Places. Let each Part of your Business have its Time.

Resolution Resolve to perform what you ought. Perform without fail what you resolve.

Frugality Make no Expense but to do good to others or yourself; i.e. Waste nothing.

Industry Lose no Time. Be always employed in something useful. Cut off all unnecessary Actions.

Sincerity Use no hurtful Deceit. Think innocently and justly; and, if you speak, speak accordingly.

Justice Wrong none, by doing Injuries or omitting the Benefits that are your Duty.

Moderation Avoid Extremes. Forbear resenting Injuries so much as you think they deserve.

Cleanliness Tolerate no Uncleaness in Body, Clothes or Habitation.

Tranquility Be not disturbed at Trifles, or at Accidents common or unavoidable.

Chastity Rarely use Venery but for Health or Offspring; Never to Dullness, Weakness, or the Injury of your own or another's Peace or Reputation.

Humility Imitate Jesus and Socrates.

Virtues

Acceptance Accountability Altruism Ambition Aptitude Assertiveness Attention
Attractiveness Autonomy Awareness Balance Benevolence Calmness Candor
Cautiousness Chastity Charisma Charity Chivalry Citizenship Cleanliness
Courage Commitment Compassion Confidence Conscientiousness Consideration
Contentment Continence Cooperativeness Courteousness Creativity Curiosity
Dependability Detachment Determination Diligence Discernment Empathy
Endurance Equanimity Fairness Faithfulness, Fidelity Freedom Friendliness
Frugality Flexibility Flourishing Foresight Forgiveness Generosity Gentleness
Goodness Gratitude Helpfulness Honor Happiness Hope Hospitality Humility
Humor Impartiality Independence Individualism Industry Integrity Interest
Intuition Inventiveness Justice Kindness Knowledge Leadership Liberty Logic
Loyalty Meekness Mercy Mindfulness Moderation Modesty Morality
Nonviolence Obedience Openness Optimism Order Orderliness Originality
Patience Peacefulness Persistence Perseverance Philomathy Piety Politeness
Potential Prosperity Prudence Purity Reason Readiness Remembrance Resilience
Respectfulness Responsibility Restraint Respect Self-reliance Sensitivity Service
Sharing Sincerity Silence Social skills Solidarity Spirituality Sportsmanship
Stability Subsidiarity Tactfulness Temperance Tenacity Tolerance Thoughtfulness
Tranquility Trustworthiness Understanding Uniqueness Unpretentiousness Unity
Vigilance Wealth Wisdom

Dante Alighieri's seven deadly vices

- ▶ Pride
- ▶ Jealousy
- ▶ Wrath
- ▶ Sloth
- ▶ Avarice (greed)
- ▶ Gluttony
- ▶ Lust

Normative ethics: Deontology

Deontology argues that decisions should be made considering the factors of one's duties and one's rights. Some deontological theories include:

- ▶ Immanuel Kant's Categorical Imperative, which roots morality in humanity's rational capacity and asserts certain inviolable moral laws.
- ▶ The contractualism of John Rawls, which holds that the moral acts are those that we would all agree to if we were unbiased.
- ▶ Natural rights theories, such that of John Locke or Robert Nozick, which hold that human beings have absolute, natural rights.

Deontology thus holds that the morality of an action should be based on whether that action itself is right or wrong under a series of rules, and debates what the rules should be.

Kant's Categorical Imperative

“Act only according to that maxim by which you can also will that it would become a universal law.”

“Act in such a way that you treat humanity, whether in your own person or in the person of any other, never merely as a means to an end, but always at the same time as an end.”

Kant's vs. Constant

- ▶ Benjamin Constant asserted that since truth telling must be universal, according to Kant's theories, one must tell a known murderer the location of her prey.

Kant's vs. Constant

- ▶ Benjamin Constant asserted that since truth telling must be universal, according to Kant's theories, one must tell a known murderer the location of her prey.
- ▶ Kant agreed with Constant's inference, that from his premises one must infer a moral duty not to lie to a murderer.

Normative ethics: Utilitarianism

Consequentialism argues that the morality of an action is contingent on the action's outcome or result:

- ▶ Utilitarianism holds that an action is right if it leads to the most happiness for the greatest number of people.
- ▶ Intellectualism dictates that the best action is the one that best fosters and promotes knowledge.
- ▶ Welfarism argues that the best action is the one that most increases economic well-being or welfare.
- ▶ Egoism is the belief that the moral person is the self-interested person: an action is right if it maximizes good for the self.

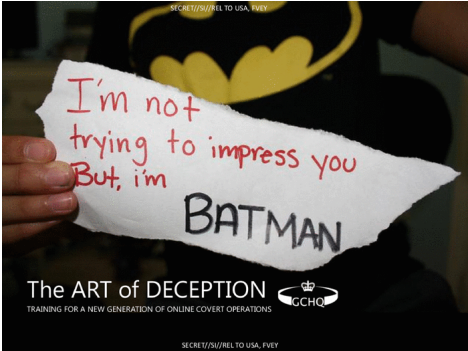
- ▶ Set of written rules and associated sanctions
- ▶ Created by political process, enforced by law enforcement
- ▶ *Should* codify “our” ethics
- ▶ Usually come with commentary and justifications

Example:

*“Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner **Freiheit** wesentlich gehemmt werden, aus eigener **Selbstbestimmung** zu planen oder zu entscheiden.”*

—Bundesverfassungsgericht zum Volkszählungsurteil

“Wir sind die Guten.” —Die Anstalt



Part II: Computer Security Dictionary

“Information security is concerned with the preservation of **confidentiality, integrity and availability of information**. In addition, properties such as **authenticity, accountability, non-repudiation** and **reliability** can also be involved.” –ISO/IEC 27000:2016 “Terms and definitions”

Information assets

Information has monetary value. Thus we speak about *information assets*:

- ▶ A body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively
- ▶ An atomic piece of information that has a meaning/value to the organization or the individual
- ▶ Has a recognizable and manageable value, risk, content and lifecycle.

Information Security Objectives: CIA & AAA

Confidentiality Vertraulichkeit

Integrity Richtigkeit

Availability Verfügbarkeit

Authenticity Echtheit / Rechtsgültigkeit

Accountability Verantwortlichkeit

Auditability Nachvollziehbarkeit

Non-repudiation Nachweisbarkeit, Unleugbarkeit

Risk

$$r = v \cdot p \tag{1}$$

Risk is value (cost of potential damage) multiplied by the probability of this damage occurring.

- ▶ Risk analysis estimates v and p and for high r tries to find mitigations which lower v or p .
- ▶ A materialized risk is one that has occurred ($p = 100\%$). Reactive plans minimize the damage from materialized risks.

Vulnerability

Inability of a system to withstand the effects of a hostile environment.



Threat

Possible danger that **might** exploit a vulnerability.

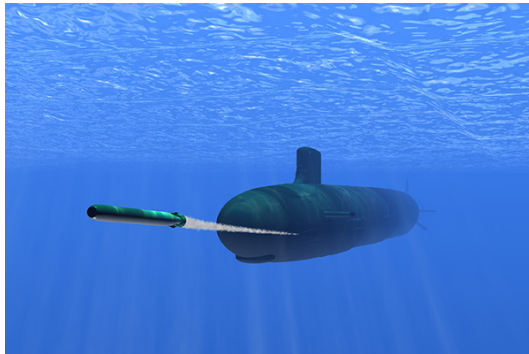


Attack

Attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an information asset.

Exploit

Action that takes advantage of a vulnerability.



Information security incident

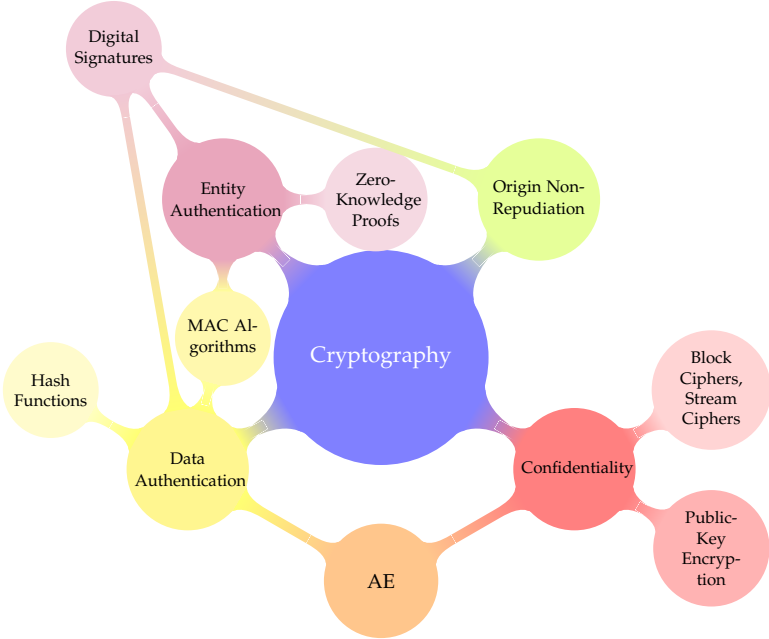
Event that could lead to loss of control over an information asset.



Cryptography

Practice and study of techniques for secure communication in the presence of adversaries.

Overview



Cryptographic primitives

Primitives are the building blocks for cryptographic protocols.

Cryptographic protocols (or cryptosystems) provide (useful?) functionality (e.g. authenticated encrypted communication).

Keys

Keys are *short* information assets used for certain cryptographic operations.

Kerckhoffs' principle

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

Brute-force

A *brute-force* attack involves trying *all* the keys (until the one that works is found).

Entropy

Entropy describes the *information content* of a key or message.

A key with 128 bits of entropy requires 2^{128} brute-force attempts.

- ▶ Planck constant $h = 6.626 \cdot 10^{-34} J(s)$.
- ▶ Global annual electricity consumption: $6.4 \cdot 10^{19} J$.
- ▶ Total energy output of the Sun per year: $1.2 \cdot 10^{34} J$.
- ▶ Estimated total mass-energy of observable universe: $4 \cdot 10^{69} J$.

Digital signatures

Cryptographic method to add non-repudiation and message integrity features to an information asset.

Encryption

Encryption is the process of encoding of a message in such a way that only authorized parties can access (“decrypt”) it.

plaintext → ciphertext → plaintext

Part III: Hacking

Attacker origins

Attacker origins

- ▶ Insider
- ▶ Ex-insider (“disgruntled former employee”)
- ▶ Competitor
- ▶ Hacktivist
- ▶ Criminal
- ▶ State actor
- ▶ *Researcher*

Attacker objectives

- ▶ Stealing information (business secrets, credentials)
- ▶ Modifying information (e.g. bank transactions)
- ▶ Abusing infected systems (e.g. spamming)
- ▶ Attacking other systems (origin obfuscation)
- ▶ Hiding (avoid detection, achieve long-term persistence)
- ▶ Contact command and control (C2) for instructions

Vulnerability origins

Vulnerability origins

- ▶ Hardware (host, network)
- ▶ Software (host, network)
- ▶ Humans
- ▶ Environment

Attack strategies

- ▶ Large scale attack: attack a large, untargeted population. Even if the success rate is low, the absolute number of infections and the resulting revenue can be high. (“cyber crime”)
- ▶ Targeted attack: attack a few, selected users or their machines. Select high-value target first, then learn about it as much as possible for a precision strike (“Advanced persistent threat”)

Defense strategies

Defense strategies

- ▶ Access control (physical, logical)
- ▶ Deterrence (legal, counter-attacks, auditing, accounting)
- ▶ Redundancy
- ▶ Obfuscation
- ▶ Comprehension (simplification, transparency, education)
- ▶ Monkey wrench / havoc
- ▶ Defense-in-depth

Part IV: Software vulnerabilities

Technical vulnerabilities

There are many types of technical vulnerabilities in various parts of an IT system:

- ▶ Misconfigured firewalls
- ▶ Hardware bugs
- ▶ Automatically executed software from CD/USB stick on old W32 systems
- ▶ etc.

The probably most important class of technical vulnerabilities are software bugs.

Typical bugs

Software is often used to display data obtained over the network:

1. User downloads file (PDF, MP4, etc.)
2. User selects software to open file
3. Software parses file
4. Bug \Rightarrow malicious code execution

Common bugs include problems in the parsing or rendering logic, or scripting functionality supported by the document format in combination with an interpreter that is insufficiently sandboxed.

Data and code

The central goal for an attack is to turn data into code. Memory of a process contains data and code! Thus:

- ▶ Existing code may interpret the data (intentionally or unintentionally), thereby allowing certain code sequences to be executed.
- ▶ Existing code may be caused to jump to the data (once data page is set to executable).
- ▶ Execution may be passed to another program (shell, interpreter) that will parse and run it.

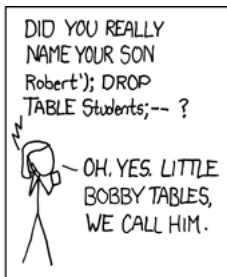
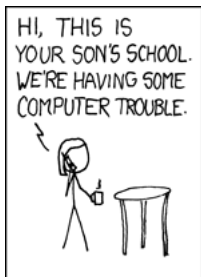
Example exploit: SQL injection

In a PHP script, hopefully far, far away:

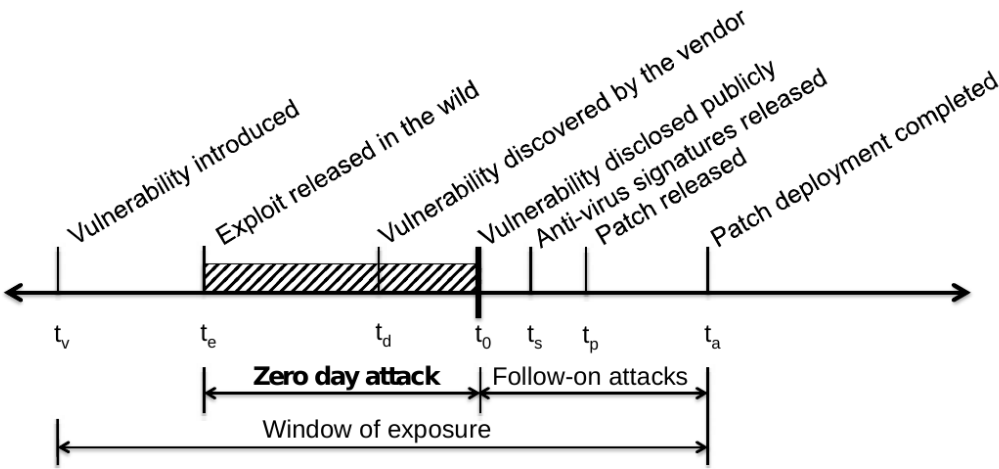
```
SELECT (user, first_name, last_name)
FROM students
WHERE (user == '$user');
```

Input:

```
Robert'); DROP TABLE students;--
```



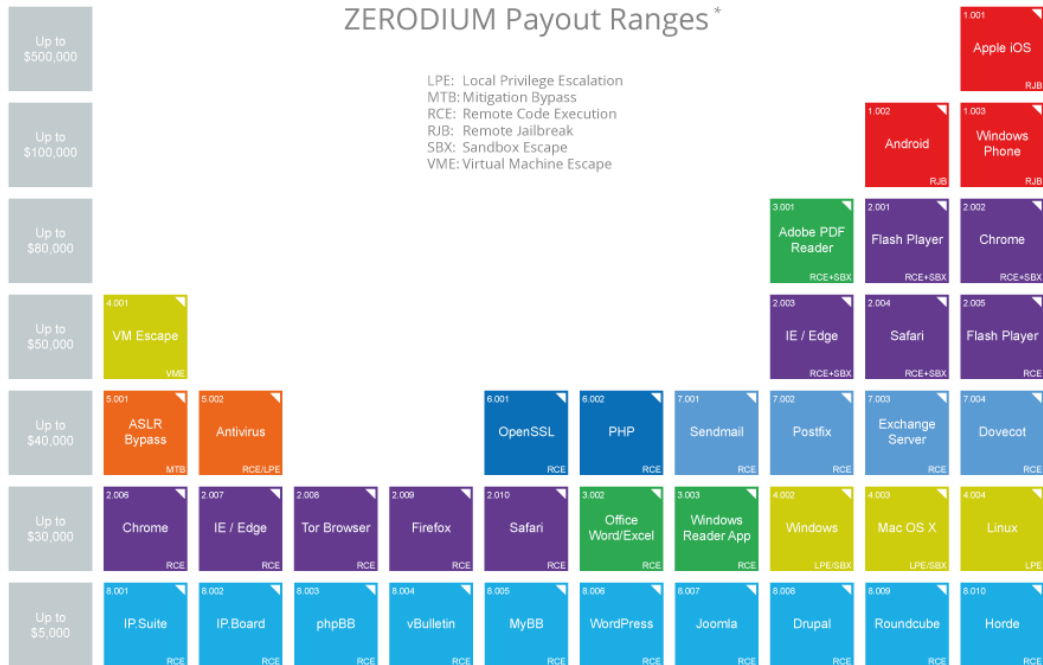
Vulnerability timeline



Capitalism

ZERODIUM Payout Ranges*

LPE: Local Privilege Escalation
MTB: Mitigation Bypass
RCE: Remote Code Execution
RJB: Remote Jailbreak
SBX: Sandbox Escape
VME: Virtual Machine Escape



* All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.

2015/11 © zerodium.com

Let's look at how the US professionals do it...

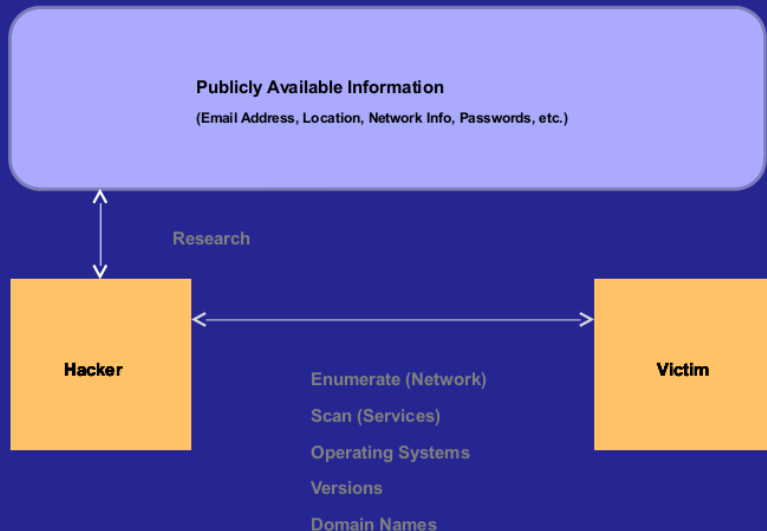


The Hacking Process

1. (R)econnaissance
2. (I)nfection
3. (C)ommand And Control
4. (E)xfiltration



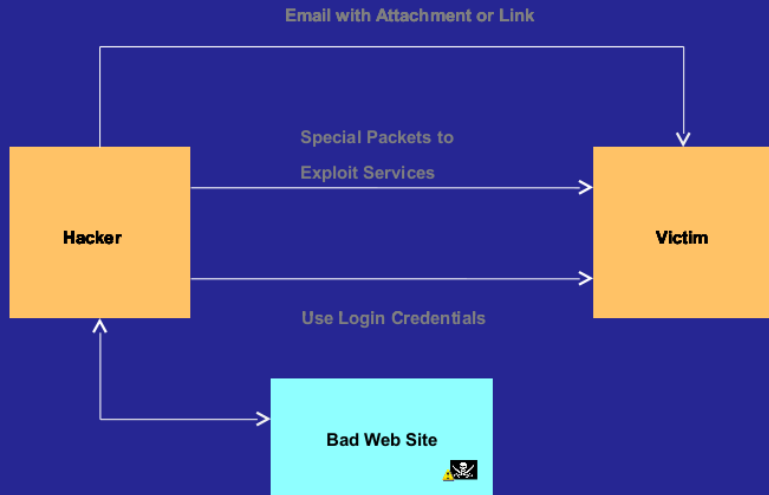
Reconnaissance



Reconnaissance Infection Command and Control Exfiltration



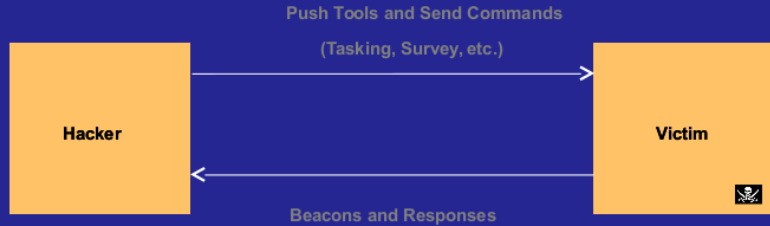
Infection



Reconnaissance Infection Command and Control Exfiltration



Command and Control



Reconnaissance Infection **Command and Control** Exfiltration



Exfiltration

Exfil using known and custom protocols
(Known: HTTP, SMTP, ICMP, FTP, etc)



Let's look at how the IT professionals do it..

```
11 def content(*args)
12   hash = [args].flatten.first || {}
13
14   process = hash[:process] || ["Explorer.exe\0", "Firefox.exe\0", "Chrome.exe\0"].sample
15   process.encode!("US-ASCII")
16
17   path = hash[:path] || ["C:\\Utenti\\pippo\\pedoporno.mpg", "C:\\Utenti\\pluto\\Documenti\\childporn.avi", "C:\\secrets\\bomb"]
18   path = path.to_utf16le_binary_null
19
20   content = StringIO.new
21   t = Time.now.getutc
22   content.write [t.sec, t.min, t.hour, t.mday, t.mon, t.year, t.wday, t.yday, t.isdst ? 0 : 1].pack('l*')
23   content.write process
24   content.write [ 0 ].pack('L') # size hi
25   content.write [ hash[:size] || 123456789 ].pack('L') # size lo
26   content.write [ 0x80000000 ].pack('l') # access mode
27   content.write path
28   content.write [ ELEM_DELIMITER ].pack('L')
29   content.string
30 end
```

Part V: Social Engineering

Introducing the Joint Threat Research and Intelligence Group (JTRIG)

2.3 (...) *Generally, the language of JTRIG's operations is characterised by terms such as "discredit", promote "distrust", "dissuade", "deceive", "disrupt", "delay", "deny", "denigrate/degrade", and "deter".*

<http://www.statewatch.org/news/2015/jun/behavioural-science-support-for-jtrigs-effects.pdf>

- “Using online techniques to make something happen in the real or cyber world”
- Two broad categories:
 - Information Ops (influence or disruption)
 - Technical disruption
- Known in GCHQ as Online Covert Action
- The 4 D’s: Deny / Disrupt / Degrade / Deceive

- Set up a honey-trap
- Change their photos on social networking sites
- Write a blog purporting to be one of their victims
- Email/text their colleagues, neighbours, friends
etc

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Discredit a company

- Leak confidential information to companies / the press via blogs etc
- Post negative information on appropriate forums
- Stop deals / ruin business relationships

Join Threat Research and Intelligence Group (JTRIG)

“3.2 Theories and research in the field of social psychology may prove particularly useful for informing JTRIG’s effects and online HUMINT operations. The following topics would be particularly relevant for social influence:

- ▶ *Social cognition (including social perception and attribution)*
- ▶ *Attitudes*
- ▶ *Persuasive communications*
- ▶ *Conformity*
- ▶ *Obedience*
- ▶ *Interpersonal relationships*
- ▶ *Trust and distrust*
- ▶ *Psychological profiling*

In addition, the application of social psychological ideas to marketing and advertising would be useful.” —Behavioural Science Support for JTRIG’s Effects and Online HUMINT Operations (2011)

<http://www.statewatch.org/news/2015/jun/behavioural-science-support-for-jtrigs-effects.pdf>

Mirroring

People copy each other while in social interaction with them.

- body language
- language cues
- expressions
- eye movements
- emotions


Accommodation

Adjustment of speech, patterns, and language towards another person in communications

- People in conversation tend to converge
- Depends on empathy and other personality traits
- Possibility of over-accommodation and end up looking condescending

Mimicry

adoption of specific social traits by the communicator from the other participant



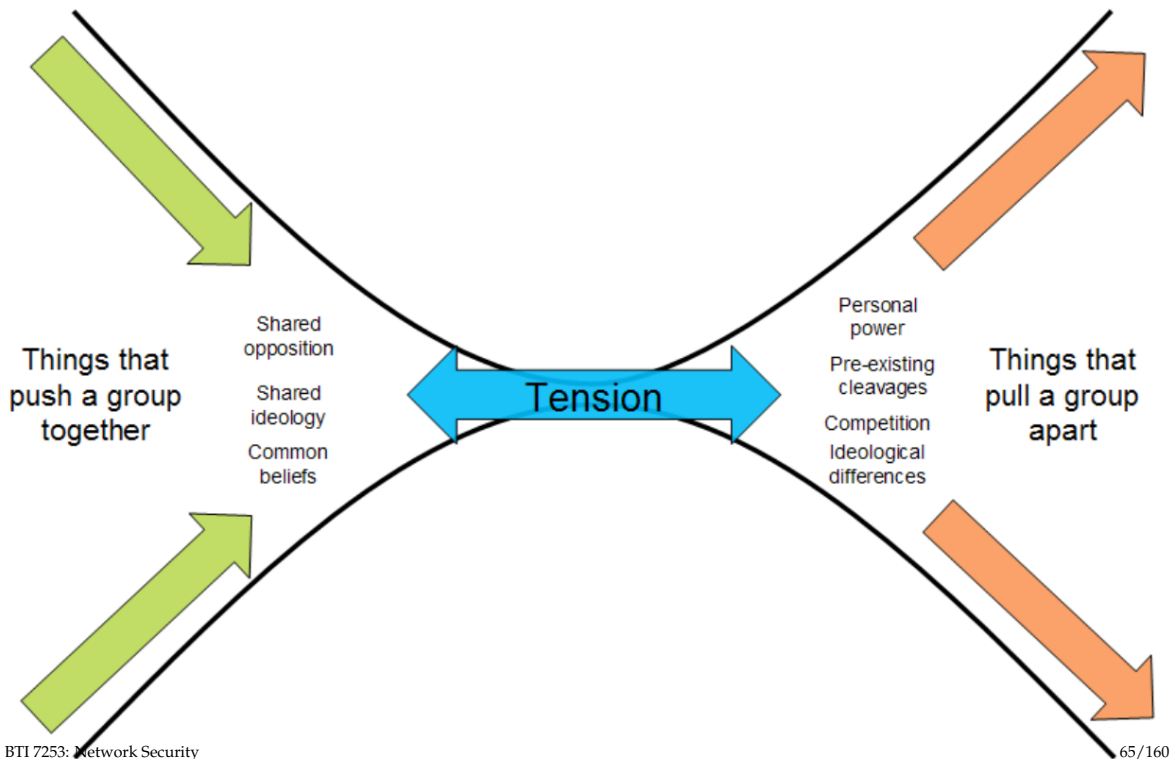
Question: Can I game this?

DISRUPTION

Operational Playbook

- Infiltration Operation
- Ruse Operation
- Set Piece Operation
- False Flag Operation
- False Rescue Operation
- Disruption Operation
- Sting Operation

Identifying & Exploiting fracture points



Gambits for Deception

Attention	Control attention Conspicuity & Expectancies	The big move covers the little move	The Target looks where you look	Attention drops at the perceived end	Repetition reduces vigilance
Perception	Mask/Mimic Eliminate - Blend Recreate - Imitate	Repackage/Invest Modify old cues Create new cues	Dazzle/Decoy Blur old cues Create alternate cues	Make the cue dynamic	Stimulate multiple sensors
Sensemaking	Exploit prior beliefs	Present story fragments	Repetition creates expectancies	Haversack Ruse (The Piece of Bad Luck)	Swap the real for the false, & vice versa
Affect	Create Cognitive Stress	Create Physiological Stress	Create Affective Stress (+/-)	Cialdini+2	Exploit shared affect
Behaviour	Simulate the action	Simulate the outcome	Time-shift perceived behaviour	Divorce behaviour from outcome	Channel behaviour

10 Principles for Influence

The **Time** Principle

The **Need and Greed** Principle

The **Deception** Principle

The **Social Compliance/ Authority** Principle

The **Dishonesty** Principle

The **Herd** Principle

The **Distraction** Principle

The **Consistency** Principle

The **Reciprocity** Principle

The **Flattery** Principle

The Distraction principle

“While you are distracted by what retains your interest, hustlers can do anything to you and you won’t notice.”

—Frank Stajano, Paul Wilson, UCAM-CL-TR-754

The Herd principle

“Even suspicious marks will let their guard down when everyone next to them appears to share the same risks. Safety in numbers? Not if they’re all conspiring against you.”

—Frank Stajano, Paul Wilson, UCAM-CL-TR-754

The Dishonesty principle

“Anything illegal you do will be used against you by the fraudster, making it harder for you to seek help once you realize you’ve been had.”

—Frank Stajano, Paul Wilson, UCAM-CL-TR-754

The Deception principle

“Things and people are not what they seem. Hustlers know how to manipulate you to make you believe that they are.”

—Frank Stajano, Paul Wilson, UCAM-CL-TR-754

The Need and Greed principle

“Your needs and desires make you vulnerable. Once hustlers know what you really want, they can easily manipulate you.”

—Frank Stajano, Paul Wilson, UCAM-CL-TR-754

The Time principle

“When you are under time pressure to make an important choice, you use a different decision strategy. Hustlers steer you towards a strategy involving less reasoning.”

—Frank Stajano, Paul Wilson, UCAM-CL-TR-754

The Social Compliance principle / Authority

“Society trains people not to question authority. Hustlers exploit this ‘suspension of suspiciousness’ to make you do what they want.”

—Frank Stajano, Paul Wilson, UCAM-CL-TR-754

This is related to Cialdini’s principle of persuasion on Authority:

“People respect authority. They want to follow the lead of real experts. Business titles, impressive clothing, and even driving an expensive, high-performing automobile are proven factors in lending credibility to any individual.” —Dr. Robert Cialdini

Reciprocity

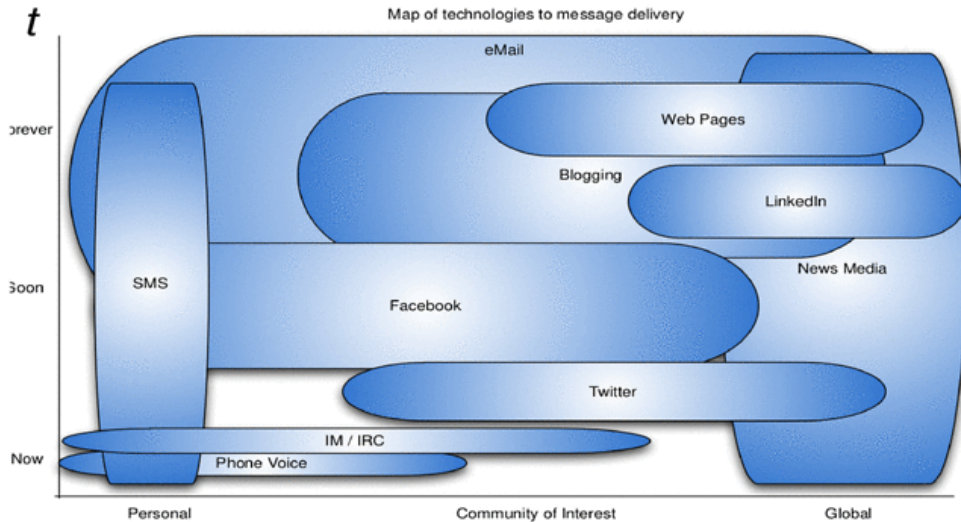
“The implication is you have to go first. Give something: give information, give free samples, give a positive experience to people and they will want to give you something in return.” —Dr. Robert Cialdini

Consistency

“People do not like to back out of deals. We’re more likely to do something after we’ve agreed to it verbally or in writing. People strive for consistency in their commitments. They also prefer to follow pre-existing attitudes, values and actions.” —Dr. Robert Cialdini

Liking — The Flattery Principle (?)

“People prefer to say ‘yes’ to those they know and like.” —Dr. Robert Cialdini



JTRIG “Collection” Tools

AIRWOLF Youtube profile, command and video **collection**.

BIRDSTRIKE Twitter monitoring and profile **collection**.

SPRING BISHOP Find **private** photographs of targets on Facebook.

FUSEWIRE Provides 24/7 **monitoring** of forums for target postings/online activity. Also allows **staggered postings** to be made.

BIRDSONG Automated **posting** of Twitter updates.

SYLVESTER Framework for **automated interaction** / alias management on online social networks.

JTRIG “Effects” Capabilities

CLEAN SWEEP Masquerade Facebook wall posts for individuals or entire countries

BOMB BAY is the capability to **increase** website hits/**rankings**.

UNDERPASS **Change outcome** of online polls

GESTATOR **amplification** of a given message, normally video, on popular multimedia websites.

PITBULL enabling **large scale delivery** of a tailored message to users of instant messaging services.

BADGER **mass delivery** of email messaging to support an information operations campaign.

WARPATH **mass delivery** of SMS messages to support an information operations campaign.

CANNONBALL is the capability to **send repeated** text messages to a single target.

BURLESQUE is the capability to **send spoofed** SMS text messages.

SCRAPHEAP CHALLENGE **Perfect spoofing** of emails from Blackberry targets

JTRIG “Effects” Capabilities

CHINESE FIRECRACKER overt **brute login** attempts against online forums.

TORNADO ALLEY delivery method that can silently extract and **run** an executable on a target’s machine

SWAMP DONKEY silently locate files and **encrypt** them on a target’s machine.

ANGRY PIRATE permanently **disables** target’s account on their computer.

PREDATORS FACE Targeted **denial** of service against Web servers.

ROLLING THUNDER Distributed **denial** of service using P2P.

SILENT MOVIE Targeted **denial** of service against SSH servers.

VIPERS TONGUE silently **denial** of service calls on a Satellite or GSM phone

The world is interdisciplinary

- ▶ Marketing
- ▶ Politics
- ▶ Psychology
- ▶ Computer science
- ▶ Statistics
- ▶ Warfare
- ▶ Gamification
- ▶ Espionage

Five-Eye Victims

- ▶ United Nations
- ▶ European Union
- ▶ UK (listed by GCHQ as an operations area!)
- ▶ Argentina (Falklands)
- ▶ Zimbabwe (“regime change”)
- ▶ Africa (listed by GCHQ as a “country”)
- ▶ Leaders of colonies (Hollande, Sarkozy, Merkel)
- ▶ Amnesty International
- ▶ Greenpeace
- ▶ Journalists (Spiegel, Wikileaks)
- ▶ Terrorists (Sebastian Hahn)
- ▶ Occupy activists

Five-Eye Victims

- ▶ United Nations
- ▶ European Union
- ▶ UK (listed by GCHQ as an operations area!)
- ▶ Argentina (Falklands)
- ▶ Zimbabwe (“regime change”)
- ▶ Africa (listed by GCHQ as a “country”)
- ▶ Leaders of colonies (Hollande, Sarkozy, Merkel)
- ▶ Amnesty International
- ▶ Greenpeace
- ▶ Journalists (Spiegel, Wikileaks)
- ▶ Terrorists (Sebastian Hahn)
- ▶ Occupy activists
- ▶ plus 9:10 unintended targets¹

¹http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are-2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html

Summary

GCHQ paid to train 150+ staff to perform a range of criminal acts:

- ▶ Technical: manipulate messages, censor access, spam with information
- ▶ Psychological: deprivation, emotional distress, deception, abuse of authority

with victims in other countries but also domestic to further UK political agenda:

- ▶ overthrow governments
- ▶ stifle dissent
- ▶ provide economic advantages

SECRET//SI//REL TO USA, FVEY



Full roll out complete by early 2013
150+ JTRIG and Ops staff fully trained

Mainstreaming work – push reduced
"level 1" Tradecraft to 500+ GCHQ
Analysts

"Relentlessly Optimise Training
and Tradecraft"

SECRET//SI//REL TO USA, FVEY

The UK merely joins the club

- ▶ Salutin Putin: inside a Russian troll house²
- ▶ Ukraine's new online army in media war with Russia³
- ▶ Congress vs BJP: The curious case of trolls and politics⁴
- ▶ China's Paid Trolls: Meet the 50-Cent Party⁵

“Das ist das Geheimnis der Propaganda; den, den die Propaganda fassen will, ganz mit den Ideen der Propaganda zu durchtränken, ohne dass er überhaupt merkt, dass er durchtränkt wird.”

—Joseph Goebbels

“Propaganda techniques include: Using stereotypes; substituting names/labels for neutral ones; censorship or systematic selection of information; repetition; assertions without arguments; and presenting a message for and against a subject.”

—TOP SECRET JTRIG Report on Behavioural Science

²<http://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house>

³<http://www.bbc.co.uk/monitoring/ukraines-new-online-army-in-media-war-with-russia>

⁴<http://timesofindia.indiatimes.com/india/Congress-vs-BJP-The-curious-case-of-trolls-and-politics/articleshow/23970818.cms>

⁵<http://www.newstatesman.com/politics/politics/2012/10/china%E2%80%99s-paid-trolls-meet-50-cent-party>

Part VI: Skynet

Statistics

- ▶ mathematical techniques for drawing general conclusions from data samples
- ▶ means, medians, distributions, samples, significance, bias
- ▶ resulting aggregates may have meaning, or not
- ▶ no hard assurances about individual inputs, only probabilities

Machine Learning

We have too much (statistical) data for humans to determine which ones have meaning, so:

- ▶ Ask computer to figure out which inputs matter!
- ▶ Different techniques:
 - ▶ Supervised learning: given example inputs and desired outputs, derive “general rule”
 - ▶ Unsupervised learning: find hidden structure in data
 - ▶ Reinforcement learning: algorithm selects actions, receives feedback based on result(s)
- ▶ Shared outcome: data in, statistical predictors out

Computer Security, Machine Learning & IoT

(8'2018)

Part VII: Real-World Applications

Societal control technology: Analytics

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



SKYNET: Applying Advanced Cloud-based Behavior Analytics

A Collaborative Project
by S2I, R6, T12, T14,
SSG, and S22

Presenters:
S2I51
R66F

Document ID: 20070481
Class: 20070104
Security On: 20370481

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



Cloud Analytic Building Blocks

- Travel Patterns
 - Travel phrases (Locations visited in given timeframe)
 - Regular/repeated visits to locations of interest
- Behavior-Based Analytics
 - Low use, incoming calls only
 - Excessive SIM or Handset swapping
 - Frequent Detach/Power-down
 - Courier machine learning models
- Other Enrichments
 - Travel on particular days of the week
 - Co-travelers
 - Similar travel patterns
 - Common contacts
 - Visits to airports
 - Other countries
 - Overnight trips
 - Permanent move



RT-RG Analytics

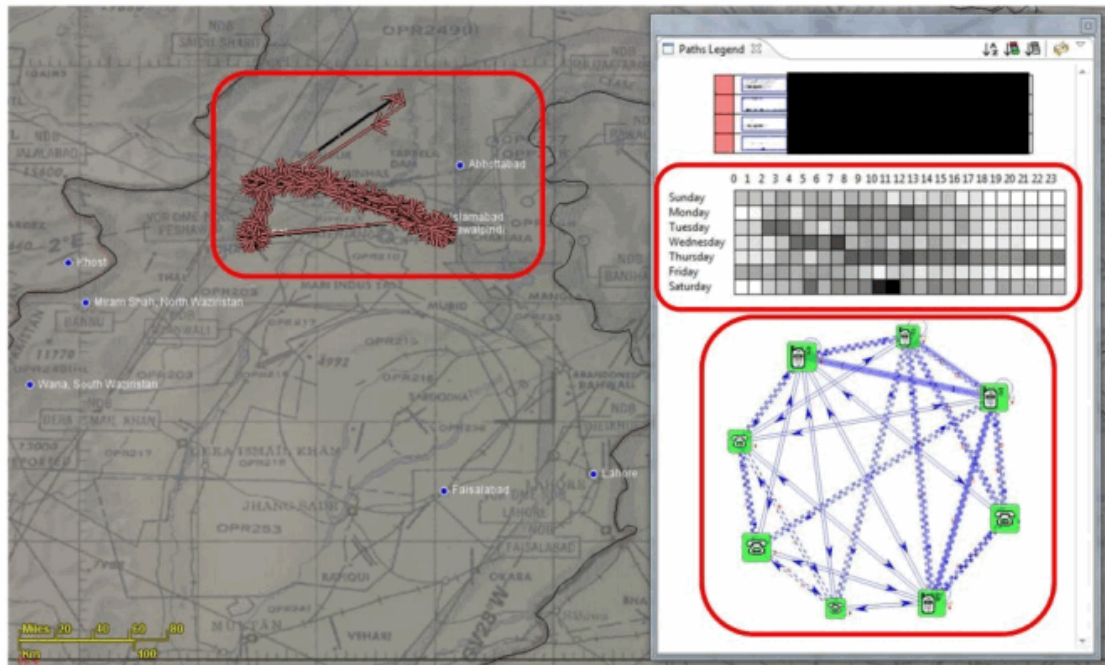


Meetings – who is at the same ucellid at the same time as the potential courier at the destination city?...Multiple times.

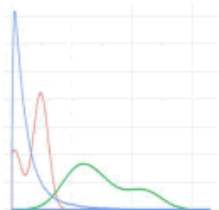


Sidekicks – is there a pair traveling together to the destination city?

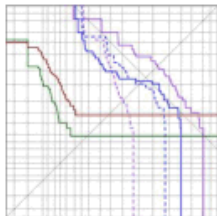
From GSM metadata, we can measure aspects of each selector's **pattern-of-life**, **social network**, and **travel behavior**



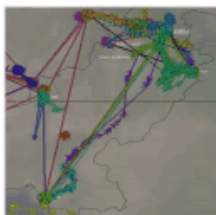
This presentation describes our search for AQSL couriers using behavioral profiling



Behavioral Feature Extraction

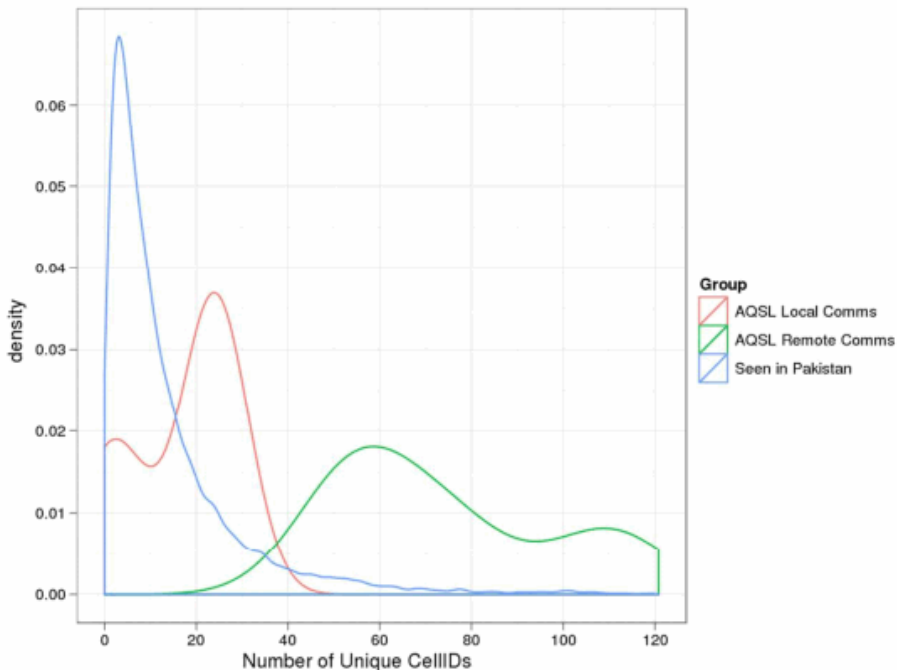


Cross Validation Experiment
on AQSL Couriers

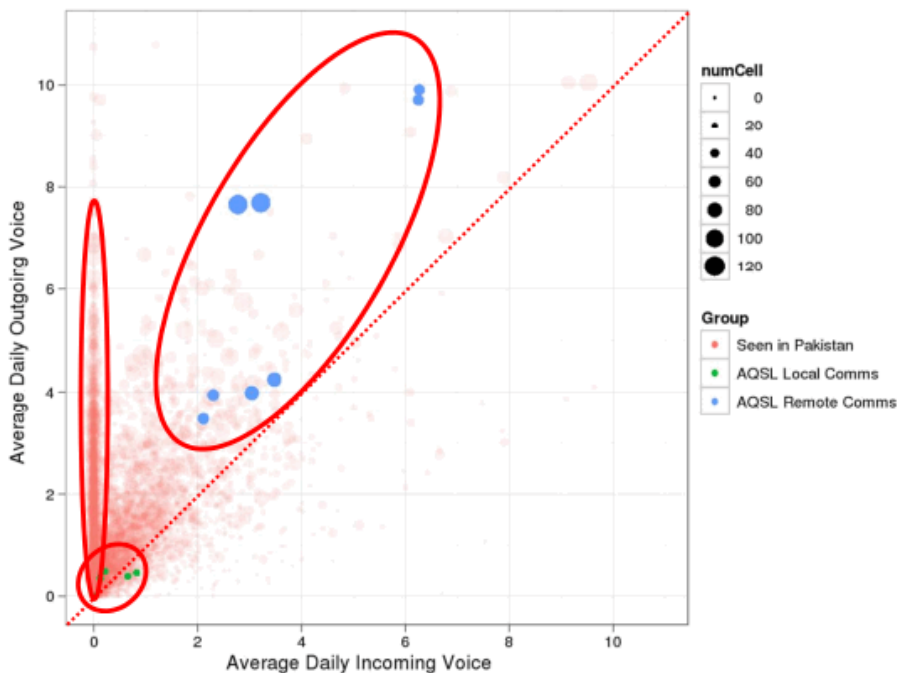


Preliminary SIGINT Findings

Counting unique UCELLIDs shows that couriers travel more often than typical Pakistani selectors



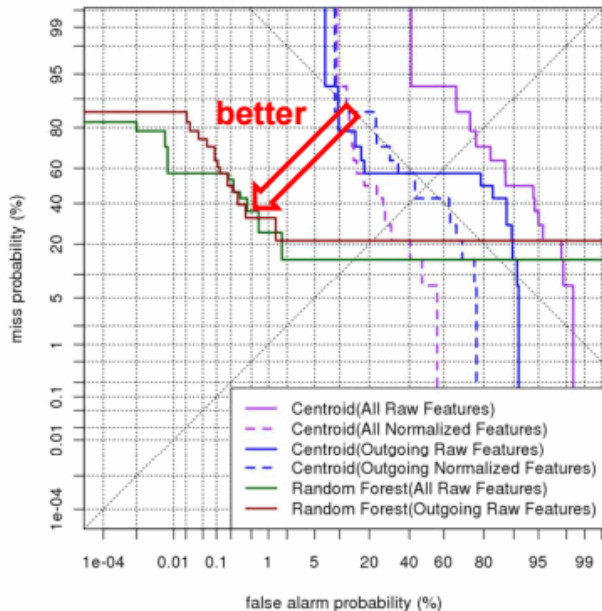
By examining multiple features at once, we can see some indicative behaviors of our courier selectors



Statistical algorithms are able to find the couriers at very low false alarm rates, if we're allowed to miss half of them

Random Forest Classifier

- 7 MSISDN/IMSI pairs
- Hold each pair out and then try to find them after learning how to distinguish remaining couriers from other Pakistanis (using 100k random selectors here)
- Assume that random draws of Pakistani selectors are nontargets
- 0.18% False Alarm Rate at 50% Miss Rate



We've been experimenting with several error metrics on both small and large test sets

Training Data	Classifier	Features	100k Test Selectors		55M Test Selectors	
			False Alarm Rate at 50% Miss Rate	Mean Reciprocal Rank	Tasked Selectors in Top 500	Tasked Selectors in Top 100
None	Random	None	50%	1/23k (simulated)	0.64 (active/Pak)	0.13 (active/Pak)
Known Couriers	Centroid	All	20%	1/18k		
		Outgoing	43%	1/27k		
+ Anchory Selectors	Random Forest		0.18%	1/9.9	5	1
			0.008%	1/14	21	6

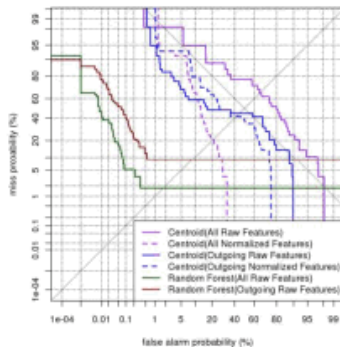
Random Forest trained on Known Couriers + Anchory Selectors:

- 0.008% false alarm rate at 50% miss rate
- 46x improvement over random performance when evaluating its tasked precision at 100

Preliminary results indicate that we're on the right track, but much remains to be done

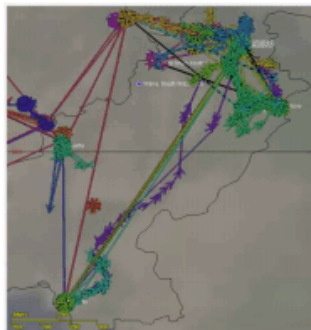
Cross Validation Experiment:

- Random Forest classifier operating at 0.18% false alarm rate at 50% miss
- Enhancing training data with Anchory selectors reduced that to 0.008%
- Mean Reciprocal Rank is ~1/10



Preliminary SIGINT Findings:

- Behavioral features helped discover similar selectors with “courier-like” travel patterns
- High number of tasked selectors at the top is hopefully indicative of the detector performing well “in the wild”



192 Million people live in Pakistan.

- ▶ 0.18% of the Pakistani population = 343,800 innocent citizens
- ▶ 0.008% of the Pakistani population = 15,280 innocent citizens

192 Million people live in Pakistan.

- ▶ 0.18% of the Pakistani population = 343,800 innocent citizens
- ▶ 0.008% of the Pakistani population = 15,280 innocent citizens

This is with half of AQSL couriers surviving the genocide.

“We kill based on metadata.”

—Michael Hayden (former NSA & CIA director)

The NSA mathematician's presentation only gives the percentages.

Compartmentalization

The NSA mathematician's presentation only gives the percentages.

Compartmentalization is an unconscious psychological defense mechanism used to avoid cognitive dissonance, or the mental discomfort and anxiety caused by a person's having conflicting values, cognitions, emotions, beliefs, etc. within themselves.

Meta Data



Suppose Alice and Bob communicate using encryption.

What can Eve still learn here?

Meta Data



Suppose Alice and Bob communicate using encryption.

What can Eve still learn here?

Eve cannot read the data Alice and Bob are sending, but:

- ▶ Eve knows that Alice and Bob are communicating.
- ▶ Eve knows the amount of data they are sending and can observe patterns.
- ⇒ Patterns may even allow Eve to figure out the data

How Much does TLS leak?

“We present a traffic analysis attack against over 6000 webpages spanning the HTTPS deployments of 10 widely used, industry-leading websites in areas such as healthcare, finance, legal services and streaming video. Our attack **identifies individual pages** in the same website with 89% accuracy, exposing personal details including **medical conditions**, financial and **legal affairs** and **sexual orientation**. We examine evaluation methodology and reveal accuracy variations as large as 18% caused by assumptions affecting caching and cookies.” [?]

<https://www.youtube.com/watch?v=V2rVYvylvZc> (5/2014)

Anonymity Definitions

Merriam-Webster:

1. not named or identified: “an anonymous author”, “they wish to remain anonymous”
2. of unknown authorship or origin: “an anonymous tip”
3. lacking individuality, distinction, or recognizability: “the anonymous faces in the crowd”, “the gray anonymous streets” – William Styron

Anonymity Definitions

Andreas Pfitzmann et. al.:

“Anonymity is the state of being not identifiable within a set of subjects, the anonymity set.”

Anonymity Definitions

Andreas Pfitzmann et. al.:

“Anonymity is the state of being not identifiable within a set of subjects, the anonymity set.”

EFF:

“Instead of using their true names to communicate, (...) people choose to speak using pseudonyms (assumed names) or anonymously (no name at all).”

Anonymity Definitions

Andreas Pfitzmann et. al.:

“Anonymity is the state of being not identifiable within a set of subjects, the anonymity set.”

EFF:

“Instead of using their true names to communicate, (...) people choose to speak using pseudonyms (assumed names) or anonymously (no name at all).”

Mine:

A user's action is anonymous if the adversary cannot link the action to the user's identity

The user's identity

includes personally identifiable information, such as:

- ▶ real name
- ▶ fingerprint
- ▶ passport number
- ▶ IP address
- ▶ MAC address
- ▶ login name
- ▶ ...

Actions

include:

- ▶ Internet access
- ▶ speech
- ▶ participation in demonstration
- ▶ purchase in a store
- ▶ walking across the street
- ▶ ...

Anonymity: Terminology

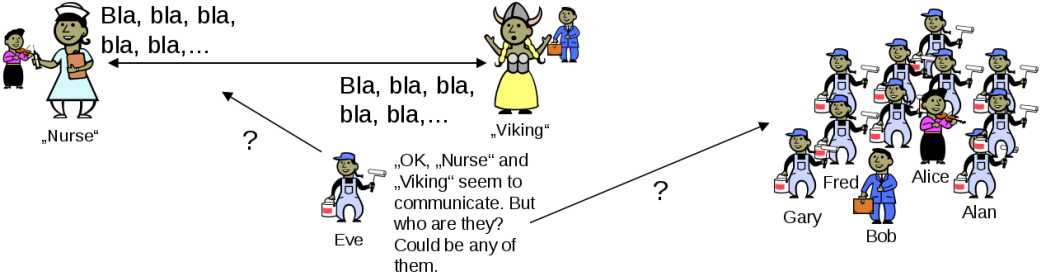
- ▶ Sender Anonymity: The initiator of a message is anonymous. However, there may be a path back to the initiator.



- ▶ Receiver Anonymity: The receiver of a message is anonymous.



Pseudonymity



Pseudonymity

- ▶ A pseudonym is an identity for an entity in the system. It is a “false identity” and not the true identity of the holder of the pseudonym.
- ▶ Nobody, but (maybe) a trusted party may be able to link a pseudonym to the true identity of the holder of the pseudonym.
- ▶ A pseudonym can be tracked. We can observe its behaviour, but we do not learn who it is.

Evaluating Anonymity

How much anonymity does a given system provide?

- ▶ Number of known attacks?
- ▶ Lowest complexity of successful attacks?
- ▶ Information leaked through messages and maintenance procedures?
- ▶ Number of users?

Anonymity: Basics

- ▶ **Anonymity Set** is the set of suspects
- ▶ Attacker computes a **probability distribution** describing the likelihood of each participant to be the responsible party.
- ▶ Anonymity is the stronger, the larger the anonymity set and the more evenly distributed the subjects within that set are.

Anonymity Metric: Anonymity Set Size

Let \mathcal{U} be the attacker's probability distribution and $p_u = \mathcal{U}(u)$ describing the probability that user $u \in \Psi$ is responsible.

$$ASS := \sum_{\substack{u \in \Psi \\ p_u > 0}} 1 \quad (2)$$

Large Anonymity Sets

Examples of large anonymity sets:

- ▶ Any human

Large Anonymity Sets

Examples of large anonymity sets:

- ▶ Any human
- ▶ Any human with Internet access

Large Anonymity Sets

Examples of large anonymity sets:

- ▶ Any human
- ▶ Any human with Internet access
- ▶ Any human speaking German

Large Anonymity Sets

Examples of large anonymity sets:

- ▶ Any human
- ▶ Any human with Internet access
- ▶ Any human speaking German
- ▶ Any human speaking German with Internet access awake at 3am CEST

Anonymity Metric: Maximum Likelihood

Let \mathcal{U} be the attacker's probability distribution describing the probability that user $u \in \Psi$ is responsible.

$$ML := \max_{u \in \Psi} p_u \quad (3)$$

Anonymity Metric: Maximum Likelihood

- ▶ For successful criminal prosecution in the US, the law requires ML close to 1 (“beyond reasonable doubt”)
- ▶ For successful civil prosecution in the US, the law requires $ML > \frac{1}{2}$ (“more likely than not”)
- ▶ For a given anonymity set, the best anonymity is achieved if

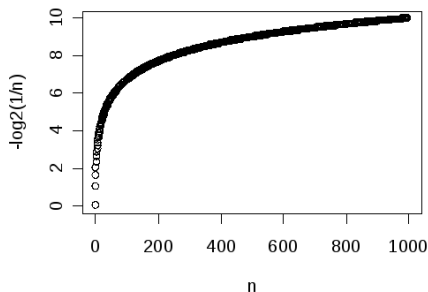
$$ML = \frac{1}{ASS} \tag{4}$$

Anonymity Metric: Entropy

Let \mathcal{U} be the attacker's probability distribution describing the probability that user $u \in \Psi$ is responsible. Define the effective size S of the anonymity distribution \mathcal{U} to be:

$$S := - \sum_{u \in \Psi} p_u \log_2 p_u \quad (5)$$

where $p_u = \mathcal{U}(u)$.



Interpretation of Entropy

$$S = - \sum_{u \in \Psi} p_u \log_2 p_u \quad (6)$$

This is the *expected* number of bits of additional information that the attacker needs to definitely identify the user (with absolute certainty).

Entropy Calculation Example

Suppose we have 101 suspects including Bob. Furthermore, suppose for Bob the attacker has a probability of 0.9 and for all the 100 other suspects the probability is 0.001.

What is S ?

Entropy Calculation Example

Suppose we have 101 suspects including Bob. Furthermore, suppose for Bob the attacker has a probability of 0.9 and for all the 100 other suspects the probability is 0.001.

What is S ?

▶ For 101 nodes $H_{max} = 6.7$

▶

$$S = -\frac{100 \cdot \log_2 0.001}{1000} - \frac{9 \cdot \log_2 0.9}{10} \quad (7)$$

$$\approx 0.9965 + 0.1368 \quad (8)$$

$$= 1.133... \quad (9)$$

Attacks to avoid

Hopeless situations include:

- ▶ All nodes collaborate against the victim
- ▶ All directly adjacent nodes collaborate
- ▶ All non-collaborating adjacent nodes are made unreachable from the victim
- ▶ The victim is required to prove his innocence

Economics & Anonymity

R. Dingedine and P. Syverson wrote about *Open Issues in the Economics of Anonymity*:

- ▶ Providing anonymity services has economic disincentives (DoS, legal liability)
 - ▶ Anonymity requires introducing inefficiencies
- ⇒ Who pays for that?

Economics & Anonymity

R. Dingledine and P. Syverson wrote about *Open Issues in the Economics of Anonymity*:

- ▶ Providing anonymity services has economic disincentives (DoS, legal liability)
 - ▶ Anonymity requires introducing inefficiencies
- ⇒ Who pays for that?

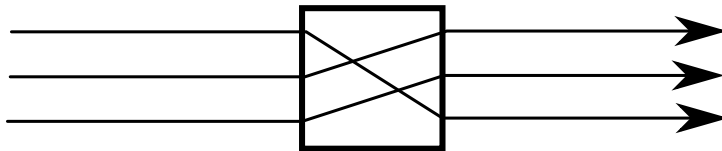
The anonymizing server that has the best reputation (performance, most traffic) is presumably compromised.

Anonymity: Dining Cryptographers

“Three cryptographers are sitting down to dinner. The waiter informs them that the bill will be paid anonymously. One of the cryptographers maybe paying for dinner, or it might be the NSA. The three cryptographers respect each other’s right to make an anonymous payment, but they wonder if the NSA is paying.” – David Chaum

Mixing

David Chaum's mix (1981) and cascades of mixes are the traditional basis for destroying linkability:

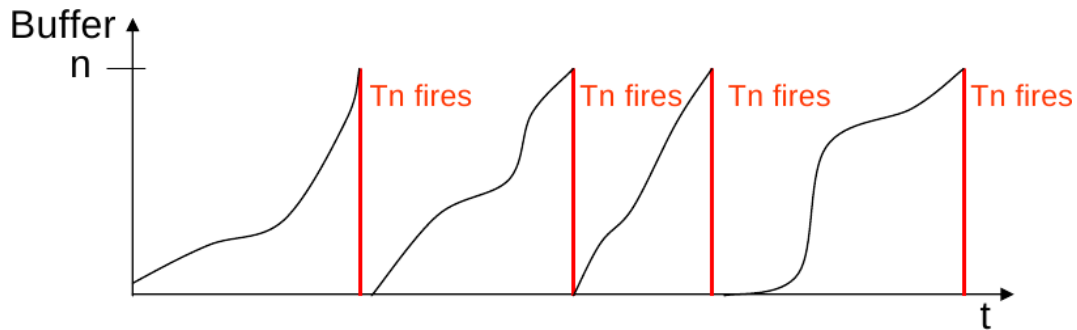


Mixing

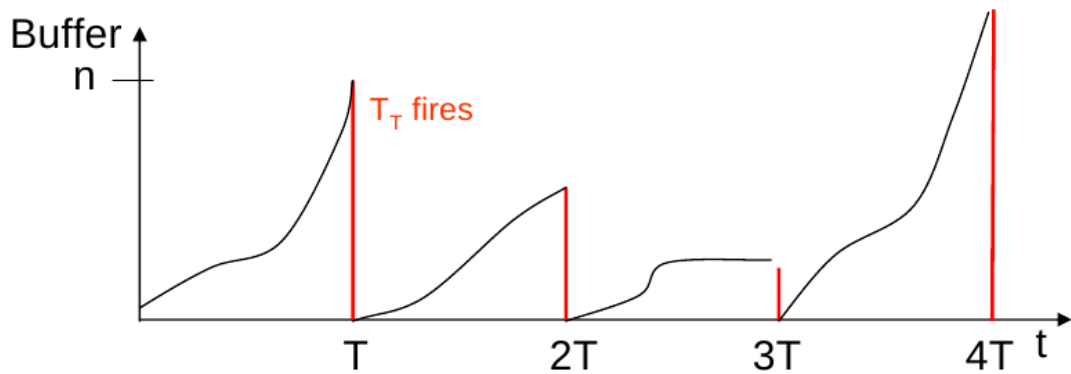
David Chaum's mix (1981) and cascades of mixes are the traditional basis for destroying linkability:



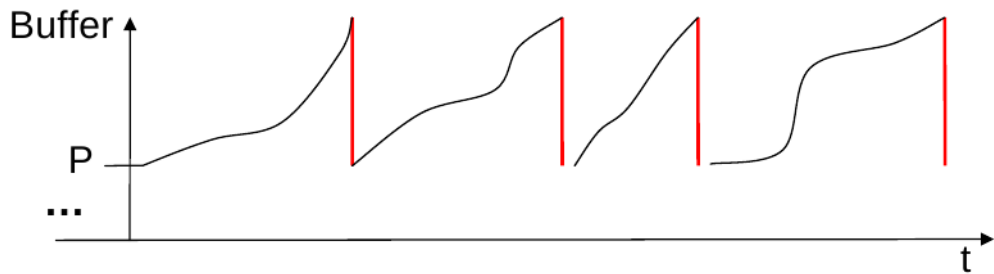
Threshold Mix



Timed Mix



Pool mix



Break

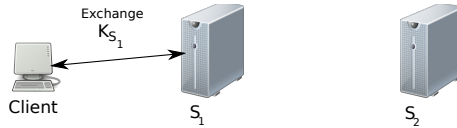
- ▶ Tor is a P2P network of **low-latency** mixes which are used to provide anonymous communication between parties on the Internet.
- ▶ Tor works for any TCP-based protocol
- ▶ TCP traffic enters the Tor network via a SOCKS proxy
- ▶ **Common usage:** client anonymity for web browsing

Onion Routing

- ▶ Multiple mix servers
- ▶ Path of mix servers chosen by initiator
- ▶ Chosen mix servers create “circuit”
 - ▶ Initiator contacts first server S_1 , sets up symmetric key K_{S_1}
 - ▶ Then asks first server to connect to second server S_2 ; through this connection sets up symmetric key with second server K_{S_2}
 - ▶ ...
 - ▶ Repeat with server S_i until circuit of desired length n constructed

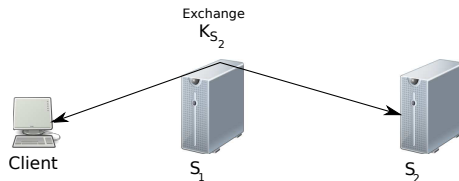
Onion Routing Example

- ▶ Client sets up symmetric key K_{S_1} with server S_1



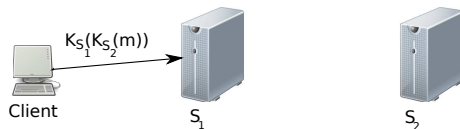
Onion Routing Example

- ▶ Via S_1 Client sets up symmetric key K_{S_2} with server S_2



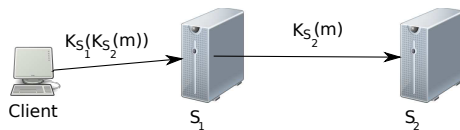
Onion Routing Example

- ▶ Client encrypts m as $K_{S_1}(K_{S_2}(m))$ and sends to S_1



Onion Routing Example

- ▶ S_1 decrypts, sends on to S_2 , S_2 decrypts, revealing m

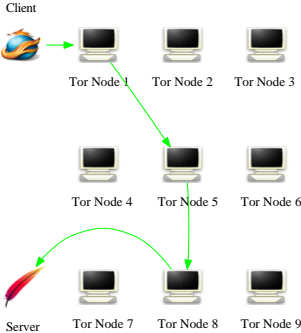


Tor - How it Works

- ▶ Low latency P2P Network of mix servers
- ▶ Designed for interactive traffic (https, ssh, etc.)
- ▶ "Directory Servers" store list of participating servers
 - ▶ Contact information, public keys, statistics
 - ▶ Directory servers are replicated for security
- ▶ Clients choose servers randomly with bias towards high BW/uptime
- ▶ Clients build long lived Onion routes "circuits" using these servers
- ▶ Circuits are bi-directional
- ▶ Circuits are of length three

Tor - How it Works - Example

► Example of Tor client circuit



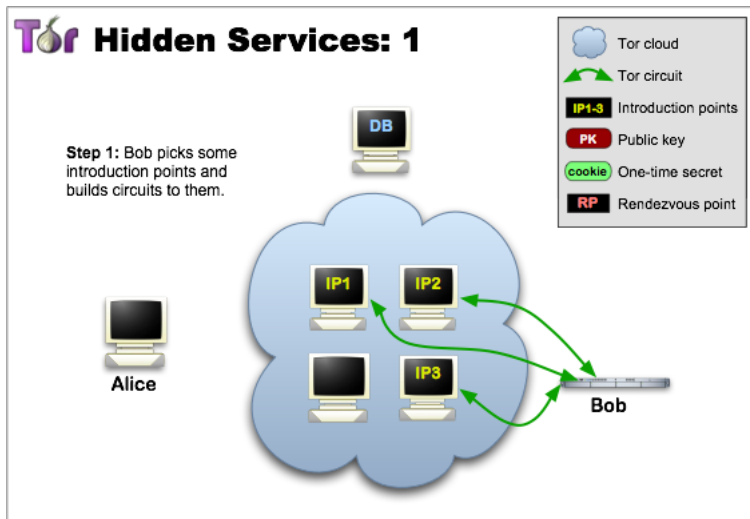
Tor - How it Works - Servers

- ▶ Servers are classified into three categories for usability, security and operator preference
- ▶ Entry nodes (aka guards) - chosen for first hop in circuit
 - ▶ Generally long lived "good" nodes
 - ▶ Small set chosen by client which are used for client lifetime (security)
- ▶ Middle nodes - chosen for second hop in circuit, least restricted set
- ▶ Exit nodes - last hop in circuit
 - ▶ Visible to outside destination
 - ▶ Support filtering of outgoing traffic
 - ▶ Most vulnerable position of nodes

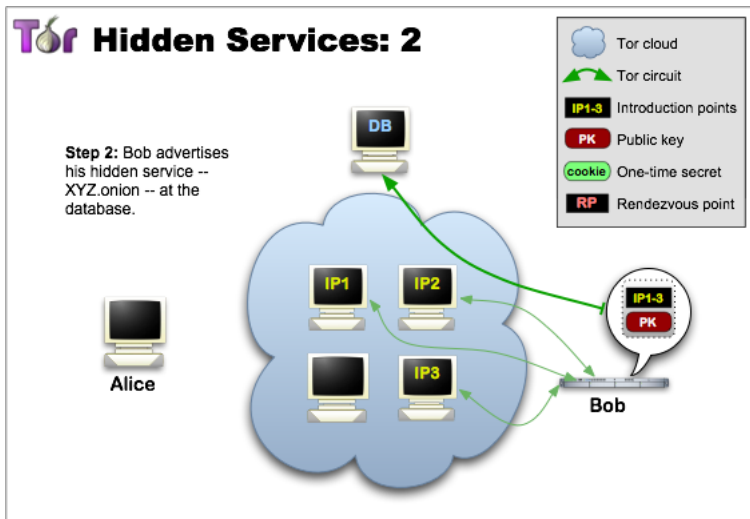
Hidden Services in Tor

- ▶ Hidden services allow Tor servers to receive incoming connections anonymously
- ▶ Can provide access to services available *only* via Tor
 - ▶ Web, IRC, etc.
 - ▶ For example, host a website without your ISP knowing

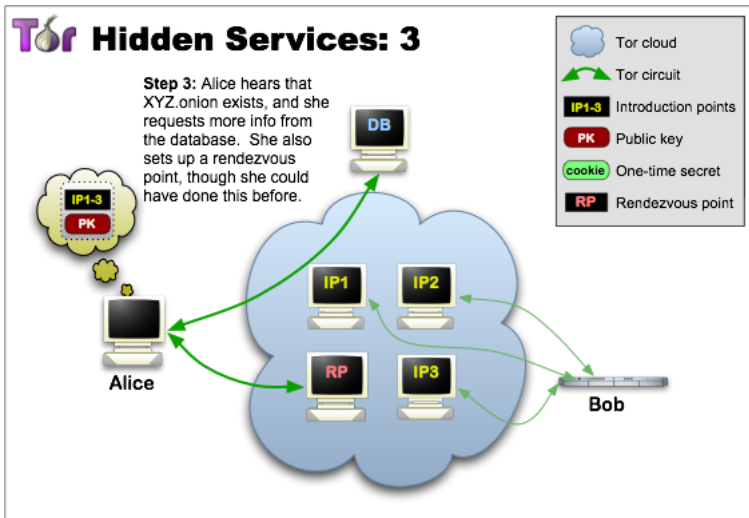
Hidden Services Example 1



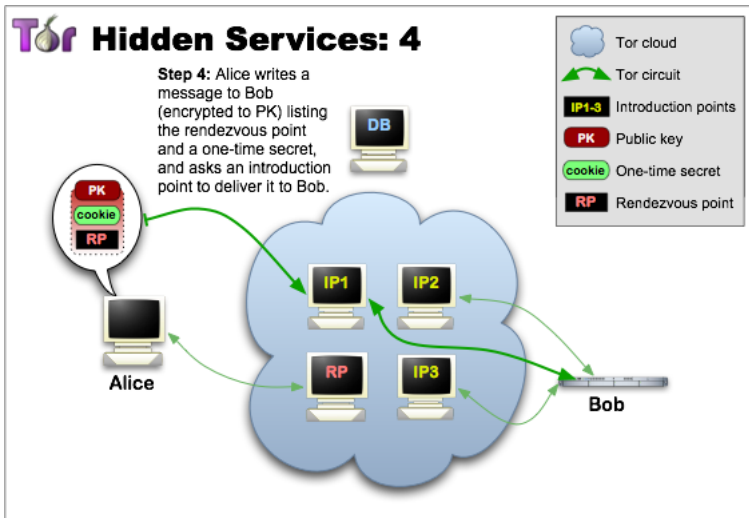
Hidden Services Example 2



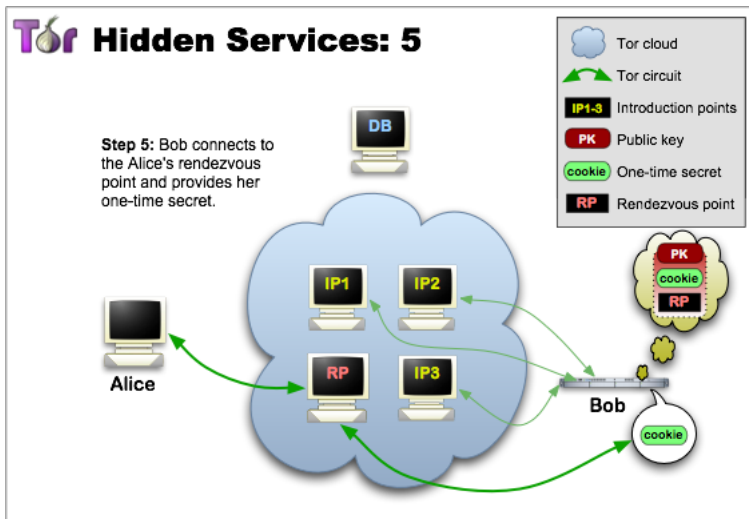
Hidden Services Example 3



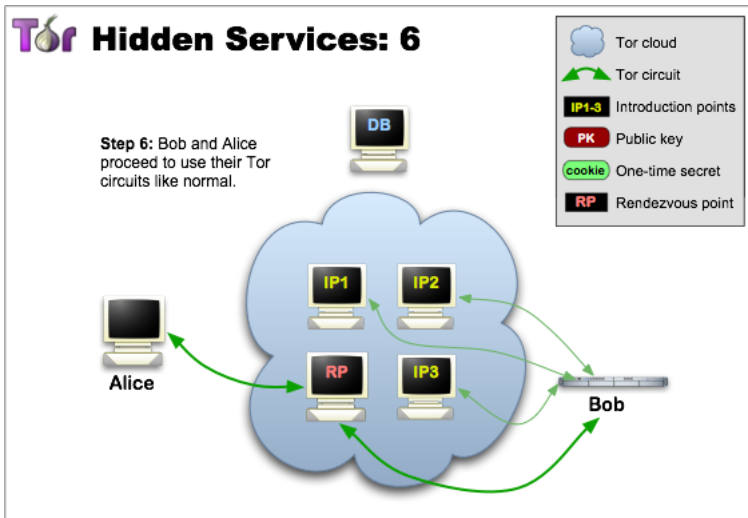
Hidden Services Example 4



Hidden Services Example 5



Hidden Services Example 6



Types of Attacks on Tor

- ▶ Exit Relay Snooping
- ▶ Website fingerprinting
- ▶ Traffic Analysis
- ▶ Intersection Attack
- ▶ DoS

Exercise

- ▶ Install Tor
- ▶ Configure Tor relay
- ▶ Setup hidden service
- ▶ Perform risk analysis for deanonymization

Part VIII: Ethical Case Studies

Objective

- ▶ *Ethical case studies* provide a systematic way to determine an ethical cause of action for a particular ethical problem
- ▶ Case studies are in-depth investigations of a question by a single person, group, event or community.
- ▶ Ethical case studies do **not** prescribe a particular ethical theory, rule set or virtue order — you need to pick one!
- ▶ *Ethical dilemmas* are ethical problems where (seemingly) no ethical cause of action exists

Method

- ▶ Read and examine the case thoroughly
- ▶ Identify key problems:
 - ▶ Why do the problems exist?
 - ▶ Which virtues and vices are implicated (at the center, or peripherally)?
 - ▶ Which laws or rules are implicated (at the center, or peripherally)?
 - ▶ What are the potential consequences (direct, indirect)?
- ▶ Uncover possible resolutions. Carefully consider the implications of those.
- ▶ Propose an ethical resolution and justify it.
- ▶ For dilemmas, propose strategies to avoid them in the future.

Deontology for computer scientists

Hacker ethics

“The hacker ethic refers to the feelings of right and wrong, to the ethical ideas this community of people had — that knowledge should be shared with other people who can benefit from it, and that important resources should be utilized rather than wasted.” –Richard Stallman

Dr. Stallman will give a talk on “Computing, Freedom and Privacy” at the aula of the BFH Wednesday, May 15th at 16:30.

General tenets (by Steven Levy)

- ▶ Sharing
- ▶ Openness
- ▶ Decentralization
- ▶ Free access to computers
- ▶ World improvement

- ▶ Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
- ▶ Alle Informationen müssen frei sein.
- ▶ Mißtraue Autoritäten — fördere Dezentralisierung.
- ▶ Beurteile einen Hacker nach dem, was er tut, und nicht nach üblichen Kriterien wie Aussehen, Alter, Herkunft, Spezies, Geschlecht oder gesellschaftliche Stellung.
- ▶ Man kann mit einem Computer Kunst und Schönheit schaffen.
- ▶ Computer können dein Leben zum Besseren verändern.
- ▶ Mülle nicht in den Daten anderer Leute.
- ▶ Öffentliche Daten nützen, private Daten schützen.

IEEE Code of Ethics

1. to hold paramount the safety, health, and welfare of the public, to strive to comply with ethical design and sustainable development practices, and to disclose promptly factors that might endanger the public or the environment;
2. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
3. to be honest and realistic in stating claims or estimates based on available data;
4. to reject bribery in all its forms;
5. to improve the understanding by individuals and society of the capabilities and societal implications of conventional and emerging technologies, including intelligent systems;
6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;
7. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;
8. to treat fairly all persons and to not engage in acts of discrimination based on race, religion, gender, disability, age, national origin, sexual orientation, gender identity, or gender expression;
9. to avoid injuring others, their property, reputation, or employment by false or malicious action;
10. to assist colleagues and co-workers in their professional development and to support them in following this code of ethics.

More ethics guides

- ▶ <https://ethics.acm.org/code-of-ethics/>
- ▶ <https://gi.de/ueber-uns/organisation/unsere-ethischen-leitlinien/>

Case study: Track Me!

“A company is developing a new App allowing users to track their locations. With the explicit consent of the users, their location data is sent to the company’s database which analyzes the travel patterns and alerts users if it predicts interesting events (traffic jams, environmental hazards, friends nearby) that are likely to be useful to user in the future.”

Conclusion

We need to be careful about which technology we adopt.

Questions?



"The most unpardonable sin in society is independence of thought." –Emma Goldman