BTI 4201: Introduction to Information Security

Christian Grothoff

BFH

25.2.2022 & 4.3.2022

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

Part I: Ethics and Law

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 Uncleanness 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.

Law and Ethics

- ▶ 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

Commercial tools: The crime fighting genie!

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

Part II: 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

General tenets (by Steven Levy)

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

CCC Hackerethik

- ▶ 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/

Part III: Computer Security Dictionary

Information Security

"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

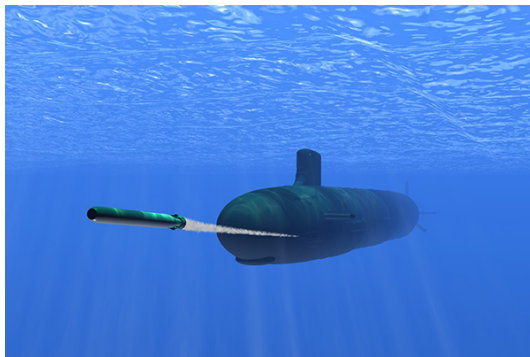Possible danger that **might** exploit a vulnerability.

Attack

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

Exploit

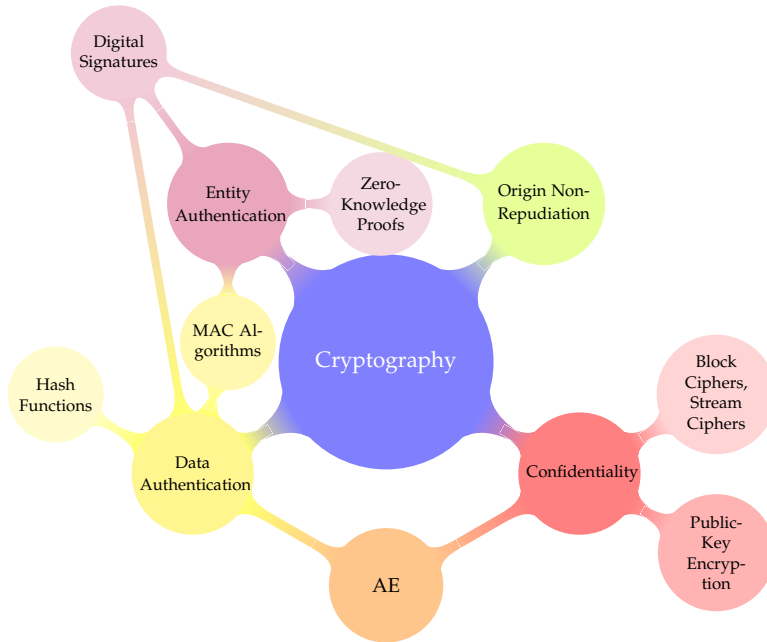Action that takes advantage of a vulnerability.

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` $\rightarrow$ `ciphertext` $\rightarrow$ `plaintext`

Attacker origins

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

Attacker objectives

- Fame
- 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

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

Banking, Surveillance and Physical Security

https://www.youtube.com/watch?v=GyJZViNf2Vk (4'2019)

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

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

Case study: (Ir)responsible disclosure

"A software developer stumbles over a potential security vulnerability. The bug itself is pretty obvious and would be trivial to fix for the original author, who is easily identified. The developer then spends a few weeks to establish that the vulnerability is indeed exploitable and develops an easy proof-of-concept exploit. Finally, they contact the author and demand that they fix the vulnerability and deploy a patch within 2 weeks after which the exploit would be released to the public."

Discuss virtues and vices affected.

Case study: (Ir)responsible disclosure

► Suppose the developer contacted the original author immediately after discovering the **potential** vulnerability, but before establishing how serious it was. Does this change your assessment?

► Suppose the developer threatened only to disclose the vulnerability to the public instead of the POC exploit. Does this change your assessment?

► Suppose the developer only disclosed the vulnerability to the author without making any threat of disclosure, resulting in the author ignoring the developer, as was to be expected by this particular author. Does this change your assessment?

► Suppose the 'author' is not a business but a volunteer providing the vulnerable software for free as a "public service". Does this change your assessment?

► Suppose the developer is Google "Project Zero" and the "author" is a Google competitor. Does this change your assessment?

Part IV: Hacking

Public Service Announcement

Special edition of the `https://nullcon.net/` security conference will be in Berlin, April 5-9th 2022.

- Student scholarships available:

    `https://nullcon.net/berlin-2022/scholarship/`

- Berlin is relatively cheap to get to and stay at[1]
- Conceivably OK to miss April 8th lectures over...

---

[1]Lufthansa Airlines discount Event code: NLZLXGO

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 probabily 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 ⇒ 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.

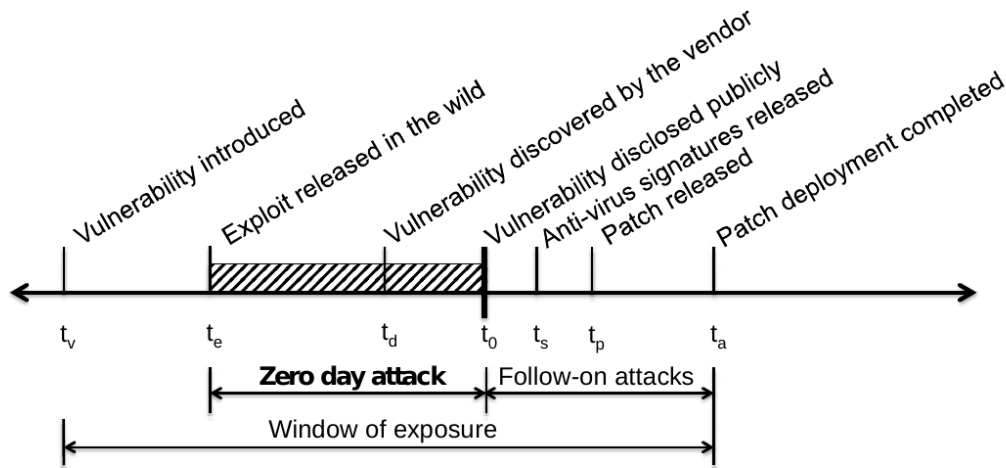# Example exploit: SQL injection

In a PHP script, hopefully far, far away:

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

Input:

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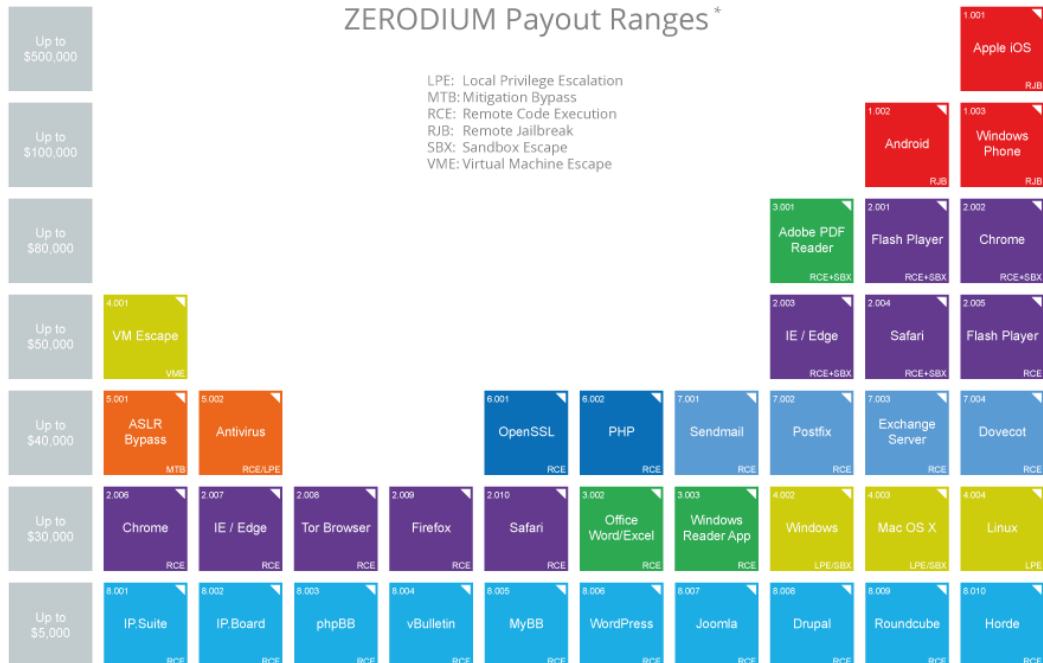
XKCD

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

Up to $500,000								1.001 Apple iOS — RJB
Up to $100,000						1.002 Android — RJB		1.003 Windows Phone — RJB
Up to $80,000						3.001 Adobe PDF Reader — RCE+SBX	2.001 Flash Player — RCE+SBX	2.002 Chrome — RCE+SBX
Up to $50,000	4.001 VM Escape — VME					2.003 IE / Edge — RCE+SBX	2.004 Safari — RCE+SBX	2.005 Flash Player — RCE
Up to $40,000	5.001 ASLR Bypass — MTB	5.002 Antivirus — RCE/LPE	6.001 OpenSSL — RCE	6.002 PHP — RCE	7.001 Sendmail — RCE	7.002 Postfix — RCE	7.003 Exchange Server — RCE	7.004 Dovecot — RCE
Up to $30,000	2.006 Chrome — RCE	2.007 IE / Edge — RCE	2.008 Tor Browser — RCE	2.009 Firefox — RCE	2.010 Safari — RCE	3.002 Office Word/Excel — RCE	3.003 Windows Reader App — RCE	4.002 Windows — LPE/SBX	4.003 Mac OS X — LPE/SBX	4.004 Linux — LPE
Up to $5,000	8.001 IP.Suite — RCE	8.002 IP.Board — RCE	8.003 phpBB — RCE	8.004 vBulletin — RCE	8.005 MyBB — RCE	8.006 WordPress — RCE	8.007 Joomla — RCE	8.008 Drupal — RCE	8.009 Roundcube — RCE	8.010 Horde — RCE

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

2015/11 © zerodium.com
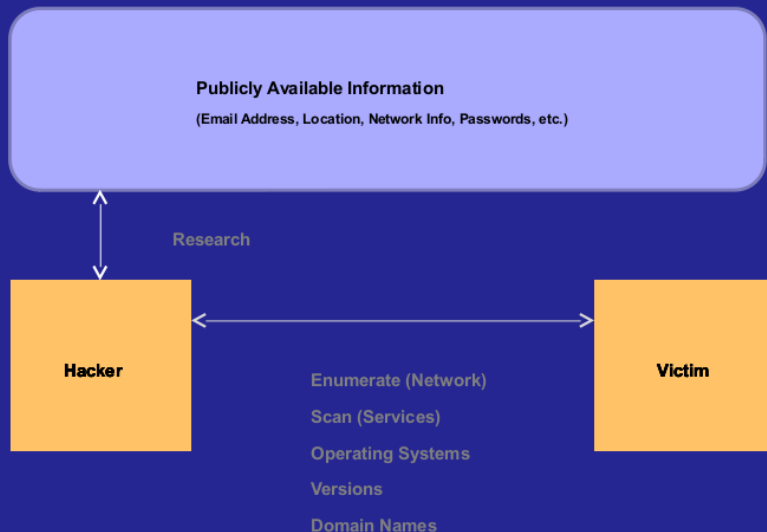
Let's look at how the US professionals do it...

The Hacking Process

1. **(R)**econnaissance
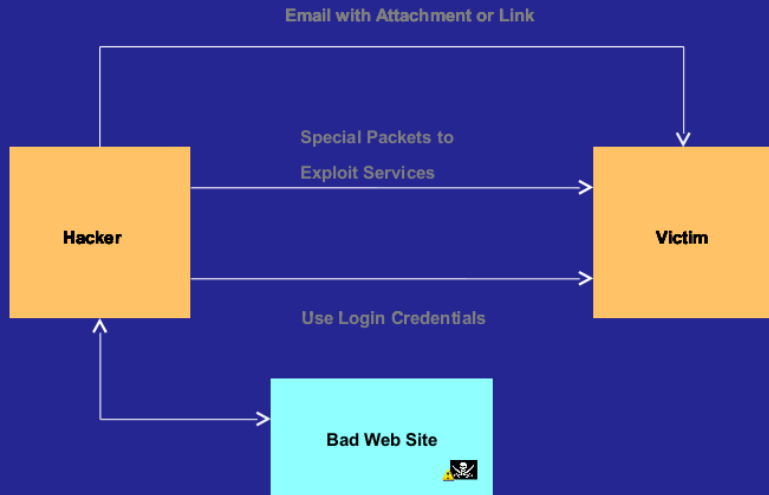
2. **(I)**nfection

3. **(C)**ommand And Control

4. **(E)**xfiltration

Reconnaissance

Publicly Available Information

(Email Address, Location, Network Info, Passwords, etc.)

Research

Hacker

Victim

Enumerate (Network)

Scan (Services)

Operating Systems

Versions

Domain Names

Reconnaissance   Infection   Command and Control   Exfiltration

Infection

Email with Attachment or Link

Special Packets to
Exploit Services

Hacker

Victim

Use Login Credentials

Bad Web Site
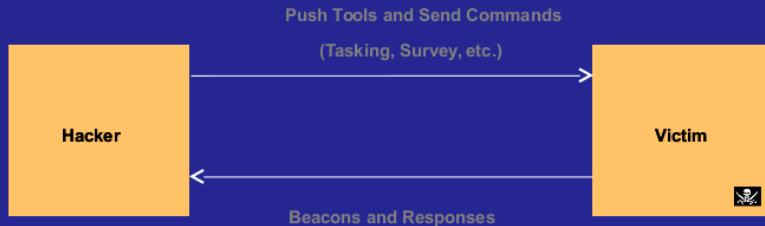
Reconnaissance   Infection   Command and Control   Exfiltration

Exfiltration

Exfil using known and custom protocols

(Known: HTTP, SMTP, ICMP, FTP, etc)

Reconnaissance   Infection   Command and Control   **Exfiltration**

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

```ruby
def content(*args)
  hash = [args].flatten.first || {}

  process = hash[:process] || ["Explorer.exe\0", "Firefox.exe\0", "Chrome.exe\0"].sample
  process.encode!("US-ASCII")

  path = hash[:path] || ["C:\\Utenti\\pippo\\pedoporno.mpg", "C:\\Utenti\\pluto\\Documenti\\childporn.avi", "C:\\secrets\\bomb_
  path = path.to_utf16le_binary_null

  content = StringIO.new
  t = Time.now.getutc
  content.write [t.sec, t.min, t.hour, t.mday, t.mon, t.year, t.wday, t.yday, t.isdst ? 0 : 1].pack('l*')
  content.write process
  content.write [ 0 ].pack('L') # size hi
  content.write [ hash[:size] || 123456789 ].pack('L') # size lo
  content.write [ 0x80000000 ].pack('l') # access mode
  content.write path
  content.write [ ELEM_DELIMITER ].pack('L')
  content.string
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
```

- 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

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
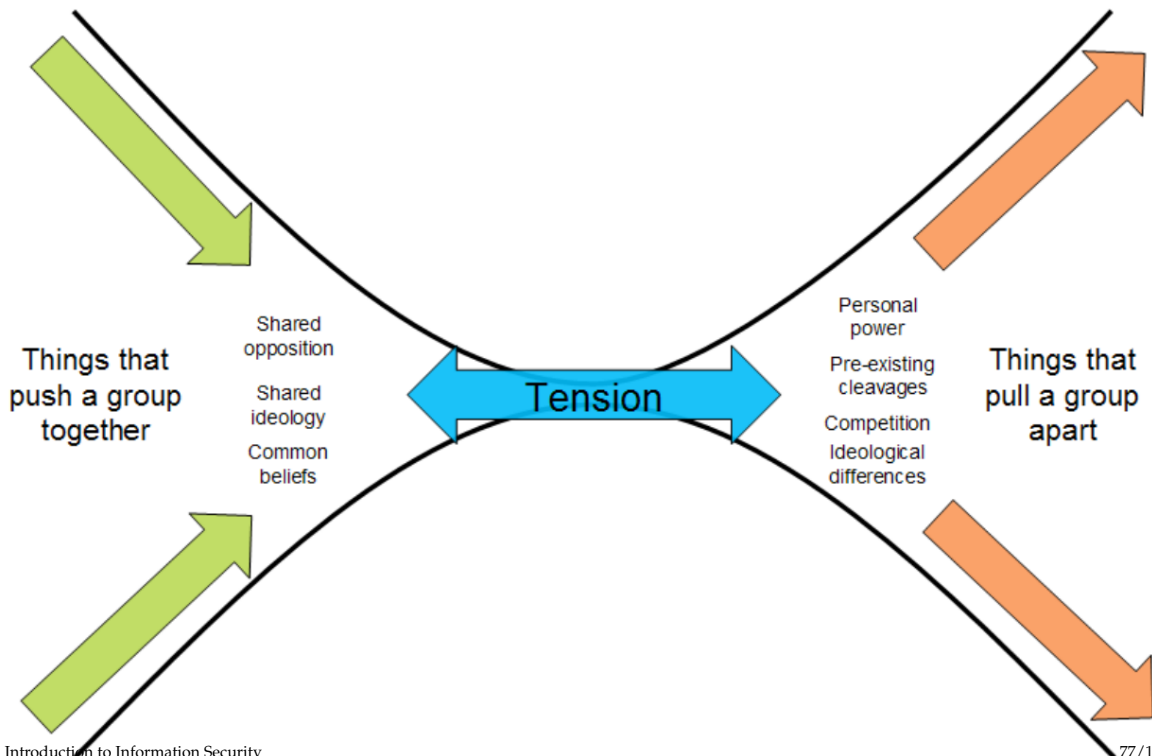
Question: Can I game this?

DISRUPTION
Operational Playbook

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

Identifying & Exploiting fracture points

Things that push a group together

Shared opposition

Shared ideology

Common beliefs

Tension

Personal power

Pre-existing cleavages

Competition

Ideological differences

Things that pull a group apart

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/Invent 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 Dishonesty Principle

The Social Compliance/ Authority 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 princple

"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

Map of technologies to message delivery
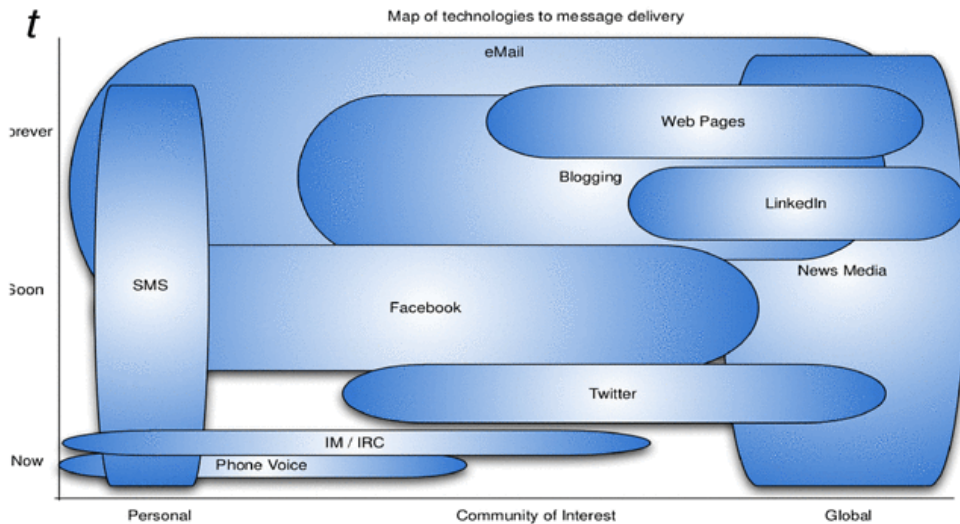
JTRIG "Collection" Tools

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)
- Torrorists (Sebastian Hahn)
- Occupy activists

2

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)
- ▶ Torrorists (Sebastian Hahn)
- ▶ Occupy activists
- ▶ plus 9:10 unintended targets[2]

---

[2]http://www.washingtonpost.com/world/national-security/
in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-ar
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: depriviation, emotional distress, deception, abuse of authority

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

- ▶ overthrow governments
- ▶ stiffle 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"

ocaa
Online Covert Action
Accreditation

SECRET//SI//REL TO USA, FVEY

The UK merely joins the club

- ▶ Salutin Putin: inside a Russian troll house[3]
- ▶ Ukraine's new online army in media war with Russia[4]
- ▶ Congress vs BJP: The curious case of trolls and politics[5]
- ▶ China's Paid Trolls: Meet the 50-Cent Party[6]

"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

---

[3]http://www.theguardian.com/world/2015/apr/02/
putin-kremlin-inside-russian-troll-house
[4]http://www.bbc.co.uk/monitoring/
ukraines-new-online-army-in-media-war-with-russia
[5]http://timesofindia.indiatimes.com/india/
Congress-vs-BJP-The-curious-case-of-trolls-and-politics/articleshow/
23970818.cms
[6]http://www.newstatesman.com/politics/politics/2012/10/china%E2%80%
99s-paid-trolls-meet-50-cent-party

Lunch break[7]

---

[7]Keep it light. The afternoon might be nauseating.

Part VI: Computer Security Research

Protocols

- "A **protocol** is a series of steps, involving two or more parties, designed to accomplish a task."
- Everyone involved must know the steps in advance and agree to follow it.
- The protocol must be complete and unambiguous.
- For cryptographic protocols, it should not be possible to do more or learn more than *what is specified in the protocol*.

Dramatis Personae

- Alice, Bob, Carol and Dave
- Eve – Eavesdropper
- Mallory – Malicious active attacker
- Trent – Trusted arbitrator
- Walter – Warden
- Peggy – Prover
- Victor – Verifier

Attack Personae

- Eavesdroppers
- Passive cheaters
- Active cheaters
- Real-world adversaries – Mallory

Efficiency

- Number of steps in protocol
- Size of messages
- Conflict resolution cost:
    1. Involvement of trusted party (arbitrated protocols)
    2. Resolution by trusted party on dispute (adjudicated protocols)
    3. Self-enforcing protocols

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
    - Reinforecment learning: algorithm selects actions, receives feedback based on result(s)
- Shared outcome: data in, statistical predictors out

Is Improving Security Possible?

(8'2018)

Part VII: Mass Surveillance

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.
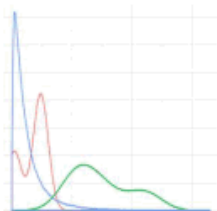

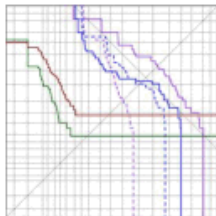Sidekicks – is there a pair traveling together to the destination city?

From GSM metadata, we can measure aspects of each selector's pattern-of-life, social network, and travel behavior
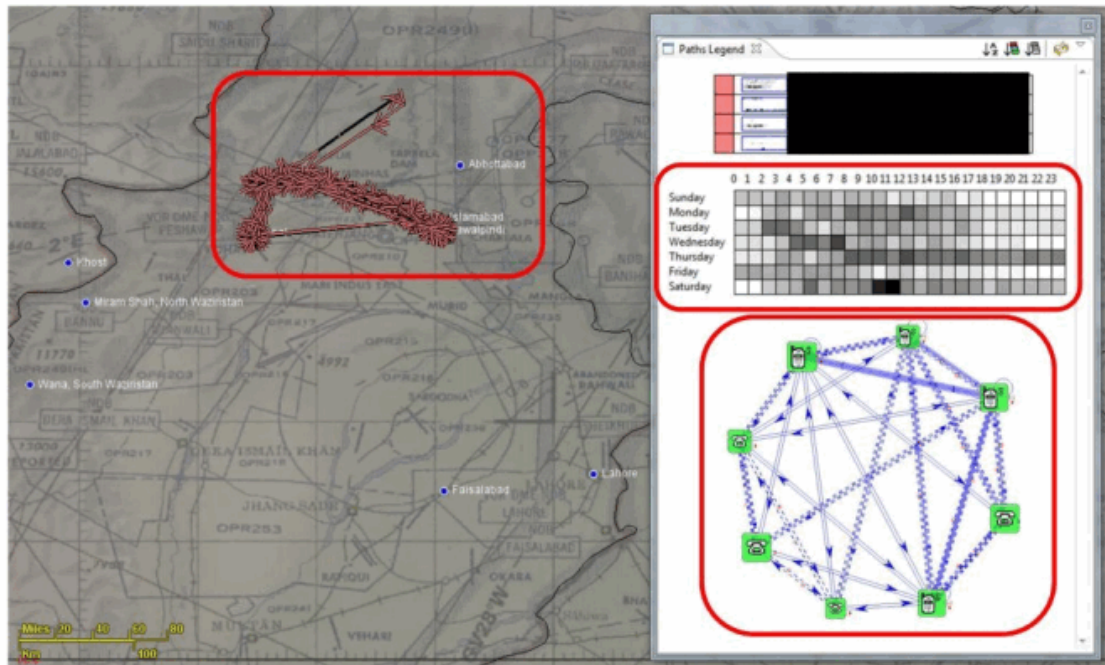
This presentation describes our search for AQSL couriers using behavioral profiling
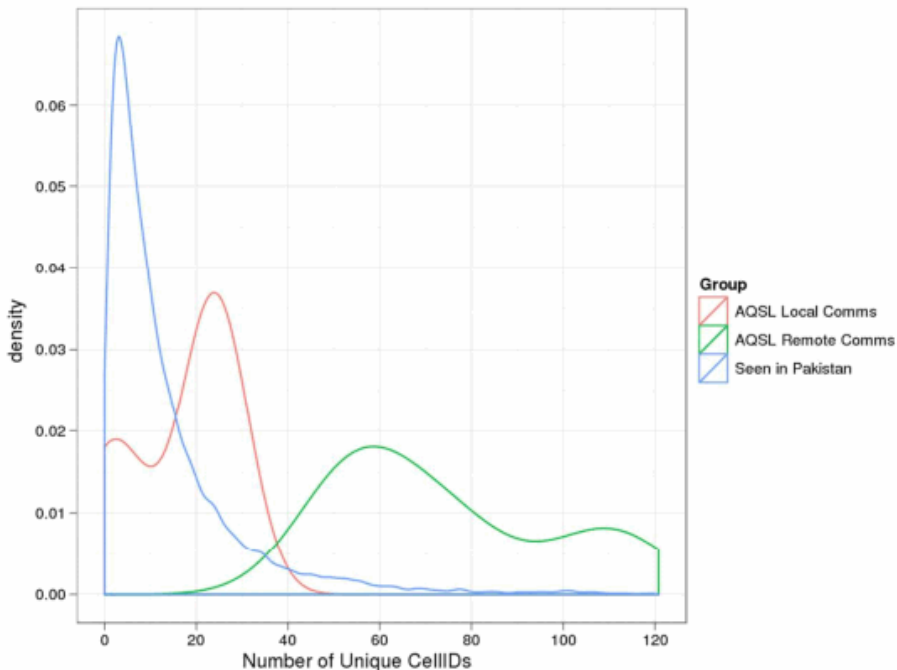

Behavioral Feature Extraction

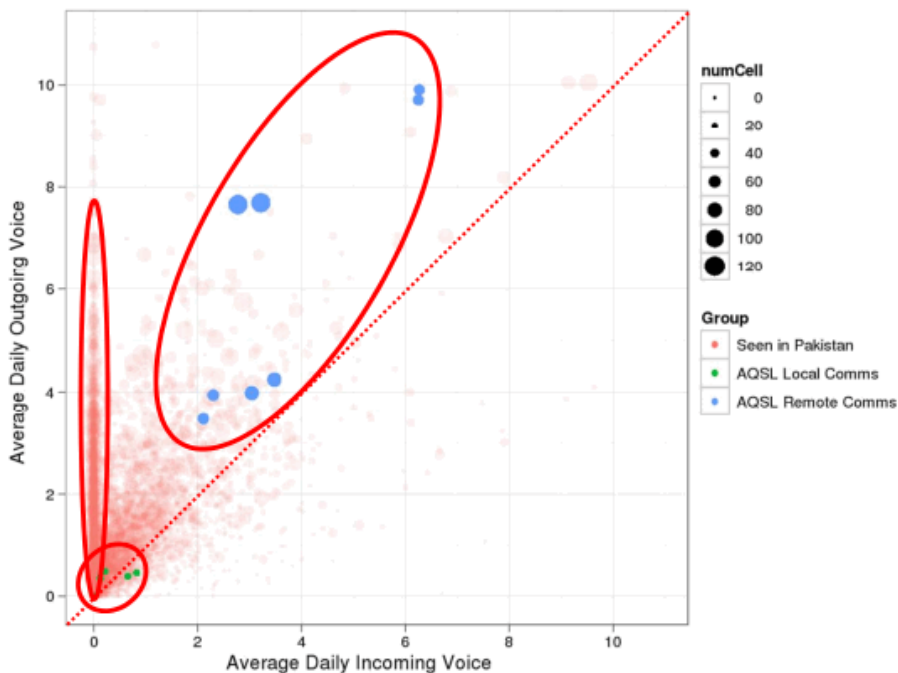Cross Validation Experiment on AQSL Couriers

Preliminary SIGINT Findings

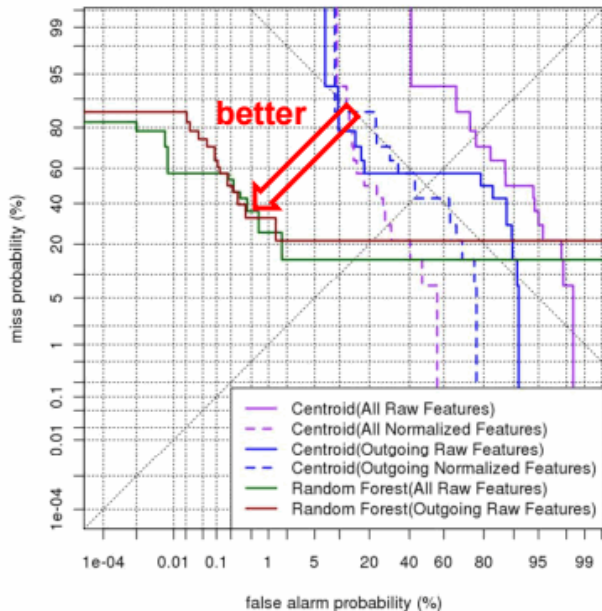# Counting unique UCELLIDs shows that couriers travel more often than typical Pakistani selectors

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

Legend:
- Centroid(All Raw Features)
- Centroid(All Normalized Features)
- Centroid(Outgoing Raw Features)
- Centroid(Outgoing Normalized Features)
- Random Forest(All Raw Features)
- Random Forest(Outgoing Raw Features)

X-axis: false alarm probability (%)
Y-axis: miss probability (%)

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		
	Random Forest		0.18%	1/9.9	5	1
+ Anchory Selectors			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
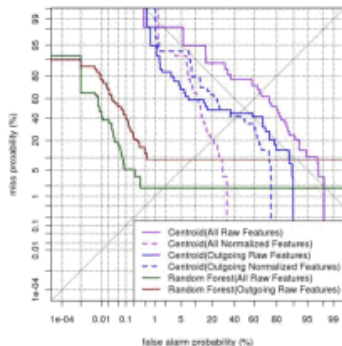
Preliminary SIGINT Findings:

- 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"
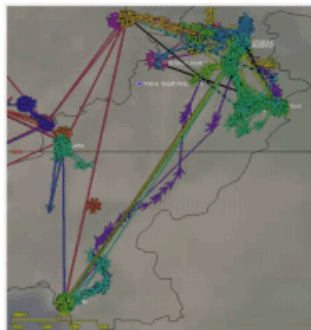
192 Million people live in Pakistan.

- ► 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.

Case study: Communication

"A company is developing new software for private communication. This will enable its customers to communicate with "complete" privacy. The solution does not include backdoors and thus the company cannot support requests for legal intercept.*"*

Case study: Private communication

- Discuss virtues and vices affected.
- Suppose the company added a "feature" to provide legal intercept support. Does this change your assessment?
- Does it make a difference if the software is "free software" developed by a community instead of proprietary software from a company?

Case study: Remote Attestation

"Researchers develop a remote attestation *method, by which a remote party (over the Internet) can tell whether some computer runs exactly the approved software configuration, and only in this case releases a decryption key. Applications for remote attestation include a broad range of copyright enforcement methods (DRM), where movies are only decoded if no recording software is detected, or where software only runs if it is properly licensed for that environment."*

Case study: Remote Attestation

- Discuss virtues and vices affected.
- Does it make a difference if this is developed for the control of military software? (Think of "copyright" enforcement for nuclear weapons launch software.)

Case study: Remote Attestation

- ▶ Discuss virtues and vices affected.
- ▶ Does it make a difference if this is developed for the control of military software? (Think of "copyright" enforcement for nuclear weapons launch software.)
- ▶ Such a mechanism is also useful to malware authors to prevent diagnosis of the malware's operation by anti-virus companies. Does this information change your assessment?

Conclusion

- Computers have no sense of ethics.
- Physical reality (including code) beats human law.

    $\Rightarrow$ We need to be careful about which technology we adopt.

Questions?

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