BTI 4202: From Secure Channels to Key Management

Christian Grothoff

Berner Fachhochschule

7.5.2021

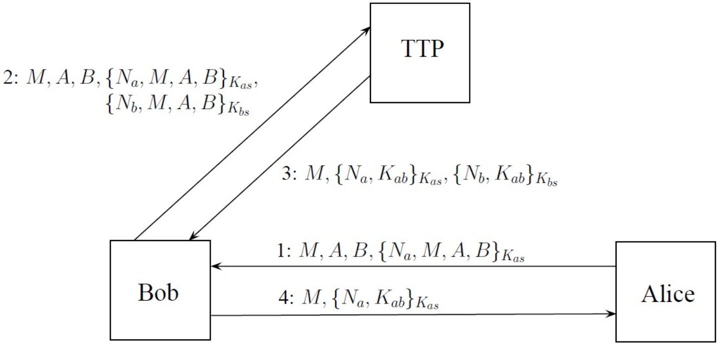
Learning Objectives

- Asynchronous secure channels
- Key Management: An Example for Architecture vulnerabilities
- Introduction to GnuPG
- Introduction to Anonymity
- Example Vulnerability: The Insecurity of WEP
- References

Homework

1. Attack against Otway-Rees protocol
2. Compromise of long term keys
3. Known session-key attacks: Kerberos and Otway-Rees
4. Attacking synchronized clock protocols: Kerberos
5. Man in the middle attack on DH

Otway-Rees protocol



Part I: Asynchronous Secure Channels

Reminder: Forward secrecy

What happens if your private key is compromised
to your *past* communication data?

Asynchronous forward secrecy: SCIMP

Idea of Silence Circle's SCIMP:

Replace key with its own hash.

- New key in zero round trips!
- Forward secrecy!

Future secrecy

Suppose your regain control over your system.
What happens with your *future* communication data?

Axolotl / Signal Protocol

```
MK        CK        RK        CK        MK
--        --        --        --        --
               ECDH(A0,B0)
                    |
                    |
     ECDH(A1,B0)    +
                   /|
                  / |
                 /  + ECDH(A1,B1)
      CK-A1-B0      |\
           |        | \
MK-0   ----+        |   \
           |        |    CK-A1-B1
MK-1   ----+        |         |
           |        |         +----  MK-0
MK-2   ----+        |         |
                    |         +----  MK-1
     ECDH(A2,B1)    +
                   /|
                  / |
                 /  |
      CK-A2-B1      |
           |        + ECDH(A2,B2)
MK-0   ----+         \
                      \
                        \
                         CK-A2-B2
                              |
```

Securing unidirectional communcation

- Alice knows Bob's public key B
- Alice wants to send M to Bob
- Alice cannot receive messages from Bob (possibly ever)

Securing unidirectional communcation

- Alice knows Bob's public key B
- Alice wants to send M to Bob
- Alice cannot receive messages from Bob (possibly ever)

Suggestion:

$$K := DH(T_A^{priv}, B) \quad (1)$$

$$C := E_K(S_A(T_A^{pub}, A, B)||M) \quad (2)$$

With Curve25519, cryptography has 92–128 bytes overhead:

- one or two 32 byte public keys
- one 64 byte EdDSA signature
- (plus HMAC)

What are the security properties we get here?

Part II: Trust Issues in X.509

Guiding questions “SSL and the Future of Authenticity”

- What is fundamentally wrong with the current CA model?
- What is the idea of “trust agility”, and is it reasonable?
- Understand the notion of “perspectives”. Evaluate strengths and weaknesses of the perspective model.

Interlude: SSL and the Future of Authenticity

Break

Part III: Introduction to GnuPG

GnuPG

- Free version of PGP, with library (libgcrypt)
- Provides common cryptographic primitives
- Provides implementation of OpenPGP (RFC 2440)
- Commonly used for secure E-mail
- Provides web of trust

Using GnuPG

```
$ gpg --gen-key
$ gpg --export
$ gpg --import FILENAME
$ gpg --edit-key EMAIL; > fpr > sign > trust
$ gpg --clearsign FILENAME
```

The Web of Trust

Problem:

- Alice has certified many of her contacts and *flagged* some as *trusted* to check keys well.
- Bob has been certified by many of his contacts.
- Alice has **not** yet certified Bob, but wants to securely communicate with him.

The Web of Trust

Problem:

- Alice has certified many of her contacts and *flagged* some as *trusted* to check keys well.
- Bob has been certified by many of his contacts.
- Alice has **not** yet certified Bob, but wants to securely communicate with him.

Solution:

- Find paths in the certification graph from Alice to Bob.
- If sufficient number of short paths exist certifying the same key, trust it.

Excercise: Explore

https://pgp.mit.edu

Break

Part IV: Introduction to Anonymity

Motivation

Suppose Alice and Bob communicate using encryption.

What can Eve still learn here?

Motivation

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.

$\Rightarrow$ 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." [1]

https://www.youtube.com/watch?v=PxwEwwlDM8Q (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:

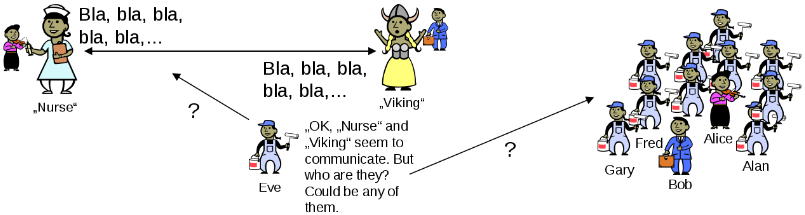
- Internet access
- speach
- participation in demonstration
- purchase in a store
- walking across the street
- ...

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 likelyhood 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.

$$ASS := \sum_{\substack{u \in \Psi \\ p_u > 0}} 1 \tag{3}$$

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.

$$ML := \max_{u \in \Psi} p_u \qquad (4)$$

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

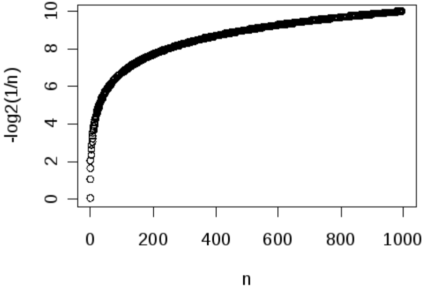
$$ML = \frac{1}{ASS} \tag{5}$$

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:

$$S := -\sum_{u \in \Psi} p_u \log_2 p_u \tag{6}$$

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



Interpretation of Entropy

$$S = -\sum_{u \in \Psi} p_u \log_2 p_u \tag{7}$$

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 $H_{max} = 6.7$
-

$$S = -\frac{100 \cdot \log_2 0.001}{1000} - \frac{9 \cdot \log_2 0.9}{10} \quad (8)$$

$$\approx 0.9965 + 0.1368 \quad (9)$$

$$= 1.133... \quad (10)$$

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. 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?

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.

Part V: Insecurity of WEP

Homework: WEP Insecurity

Read the article "Intercepting Mobile Communications: The Insecurity of 802.11" until section 4.2. For each of the attacks, decryption (section 3), message modification (section 4.1) and message injection (section 4.2) explain:

- How does the attack work?
- Why does it work (i.e., what are the flaws that make the attack possible)?

References

Brad Miller, Ling Huang, A.D. Joseph, and J.D. Tygar.
I know why you went to the clinic: Risks and realization of https traffic analysis.
http://arxiv.org/abs/1403.0297, 2014.