Leftovers: Public-Key Infrastructure

3/10/2010
Certificate Chains

Certificate:
\{\text{David Wagner’s public key is } K_{\text{Dave}}\} K^{-1}_{\text{Arnold}}

Certificate chain:
\{\text{UC Berkeley’s public key is } K_{\text{UCB}}\} K^{-1}_{\text{Arnold}}
\{\text{David Wagner’s public key is } K_{\text{Dave}}\} K^{-1}_{\text{UCB}}
Hierarchical CAs

Arnold

Cal State

U.C.

U.C. Irvine

UCB Math

David Wagner
Web of Trust

David Wagner

Vern

Christos

Bill Cheswick

Charles Stross

Neil Stephenson
SSH

First time:

SSH client

hi

$K_s$

{M}$^K_s$

SSH server

All subsequent logins:

SSH client

{M}$^K_s$

SSH server
Needham-Schroeder

{I want to talk to Bob}_KA

{I'm Alice; use k}_KB

{Use k, and send this to Bob:}

{M}_k
Alice wants to talk to Bob. She contacts a trusted server, which generates a unique key $k$ and sends it to Bob. The trusted server also sends a message encrypted with $k$ to Bob, informing him to use $k$. Bob then sends a message encrypted with $k$ back to Alice. Any other entity, such as the bad guy, trying to intercept the communication, would not be able to understand the messages due to the use of the unique key $k$.
Attacks on Cryptography

3/10/2010
Wireless networking is just radio communications

– Hence anyone with a radio can eavesdrop, inject traffic
Toys for Hackers
The Security Risk: RF Leakage
The Risk of Attack From Afar
• The industry’s solution: **WEP** (Wired Equivalent Privacy)
  – Share a single cryptographic key among all devices
  – Encrypt all packets sent over the air, using the shared key
  – Use a checksum to prevent injection of spoofed packets
WEP - A Little More Detail

- WEP uses the RC4 stream cipher to encrypt a TCP/IP packet ($P$) by xor-ing it with keystream ($\text{RC4}(K, IV)$)
A Risk of Keystream Reuse

- In some implementations, IVs repeat.
  - If we send two ciphertexts \((C, C')\) using the same IV, then the xor of plaintexts leaks \((P \oplus P' = C \oplus C')\), which might reveal both plaintexts.

Lesson: If RC4 isn’t used carefully, it becomes insecure.
WEP -- Even More Detail
Attack #2: Spoofed Packets

- Attackers can inject forged 802.11 traffic
  - Learn $Z = \text{RC4}(K, IV)$ using previous attack
  - Since the CRC checksum is unkeyed, you can then create valid ciphertexts that will be accepted by the receiver

- Attackers can bypass 802.11 access control
  - All computers attached to wireless net are exposed
Attack #3: Packet Modification

- CRC is linear
  \[\text{CRC}(P \oplus \Delta) = \text{CRC}(P) \oplus \text{CRC}(\Delta)\]
  \[\implies\] the modified packet \((P \oplus \Delta)\) has a valid checksum

- Attacker can tamper with packet \((P)\) without breaking RC4
Attack #4: Inductive Learning

- Learn $Z_{1..n} = \text{RC4}(K, IV)_{1..n}$ using previous attack
- Then guess $Z_{n+1}$; verify guess by sending a ping packet $((P, CRC(P)))$ of length $n+1$ and watching for a response
- Repeat, for $n=1,2,...$, until all of $\text{RC4}(K, IV)$ is known

Credits: Arbaugh, et al.
Attack #5: Reaction Attacks

- TCP ACKnowledgement returned by recipient
  \[ P \oplus RC4(K) \text{ (ACK)} \]
  \[ P \oplus RC4(K) \oplus 0x00010001 \]
  \[ wt(P \& 0x00010001) = 1 \]

- Attacker can recover plaintext \( P \) without breaking RC4
Wardriving / Access Point Mapping

468 WEP
1,265 Clear
1,733 Total