

Security Overview Ideas for Security Projects

Class 5
28 January 2003

Outline

- What is security?
 - Trust models
 - Attacker models
- Goal of this lecture
 - Discuss 3 security project directions
 - Paper similar to these 3 could be result of class project
- 3 papers dealing with security attacks
 - Mitigating routing misbehavior
 - Sybil attack
 - 802.11 attacks

What is Security?

- Managing a malicious adversary
- Guaranteeing properties even if a malicious adversary tries to attack
- Basic security properties
 - Authenticity
 - Integrity
 - Confidentiality
 - Availability
- Trust assumptions & security mechanisms & attacker model give security properties

Attacker Model

- Passive vs active attacker
- Usual attacks
 - Node compromise
 - Denial-of-service attacks
- Wired communication environment
 - Eavesdropping possible
 - Packet injection (source address spoofing) easy
- Wireless communication environment
 - Eavesdropping easy
 - Packet injection (source address spoofing) easy
 - Sybil attack

Mitigating Routing Misbehavior

- Ad hoc network:
 - Wireless nodes forwarding packets for other nodes to extend communication range
 - Simple network deployment without setting up an infrastructure
 - Nodes are usually mobile, network is constantly changing
- Problem: Nodes may not forward packets
 - Nodes may be malicious (DoS attack)
 - Nodes may be selfish (conserve energy)
- Proposed solution: Watchdog and Pathrater

Ad Hoc Network Routing

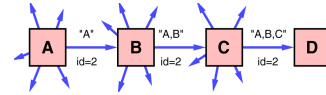


- Ad hoc network routing protocols allow communication without infrastructure
- Routes are automatically discovered and maintained

Dynamic Source Routing (DSR)

- Divides the routing problem into two parts:
 - Route Discovery:** only try to find a route to some destination when you don't have one and need one (DSR is on-demand)
 - Route Maintenance:** only while you're actually using a route, try to keep it working or fix it in spite of changes
- Properties of DSR:
 - Nodes ignore topology changes not affecting them
 - Overhead scales with increased movement

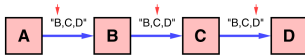
Route Discovery Overview



- Broadcast a **ROUTE REQUEST** with a unique request id
- When receiving a **ROUTE REQUEST**:
 - If target is yourself, return recorded route to initiator in a **ROUTE REPLY** packet; initiator caches route
 - Else, if recently forwarded a REQUEST with this id, drop the Request
 - Else, append your own address to a route record in the packet and rebroadcast the **ROUTE REQUEST**

Route Maintenance Overview

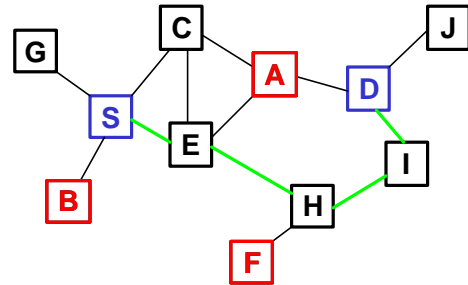
- After transmitting a packet to the next hop:
 - Listen for link-level per-hop acknowledgement, or
 - Listen for that node sending packet to its next hop, or
 - Set a bit in the packet to request an explicit next-hop acknowledgement



- When a problem with forwarding is detected:
 - Send a **ROUTE ERROR** to original sender, describing broken link
 - Sender removes the broken link from its cache

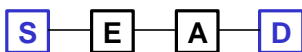
Attack Scenario

- Malicious or selfish nodes can perturb routing



Watchdog

- Detects misbehaving nodes
- Observation: Assuming bi-directional links, forwarding node can verify if following node continues to forward packet
- Example:
 - S sends packet P to D, with path E, A, D
 - After A sends P to B, A can hear when B forwards packet to C, otherwise, A believes that B is malicious

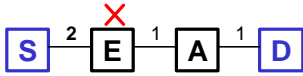


Watchdog

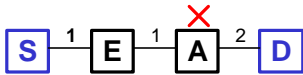
- If node drops more packets than configured minimum misbehavior threshold, watchdog informs sender of the misbehaving node
- Limitations
 - Ambiguous collisions
 - Receiver collisions
 - Limited transmission power
 - False misbehavior
 - Collusion
 - Partial dropping

Watchdog Problems

- Ambiguous collision



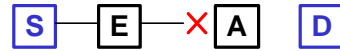
- Receiver collision



Watchdog Problems

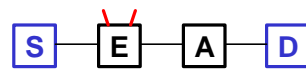
- Limited transmission power

- Or node moves out of range during send



- False misbehavior (blackmail)

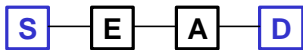
- Paper claims false report of misbehavior will be detected, e.g., E claims A is misbehaving



Watchdog Problems

- Collusion

- Paper assumes no adjacent neighbors collude, e.g., assume E & A don't collude



- Partial dropping

- Node drops at rate lower than minimum misbehavior threshold
- Not too serious: node still forwards packets

Pathrater

- Keeps rating for each node

- 1 rating for itself
- 0.5 initial rating
- Rating in [0, 0.8] for good nodes
- -100 for misbehaving nodes

- Rating updates

- +0.01 every 200ms for actively used paths
- -0.05 after link break

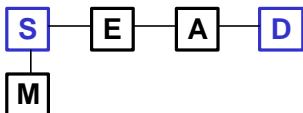
- Select path with highest average rating

- Simulates shortest path, as node itself has rating=1

Project Directions

- Solve Watchdog/Pathrater problems

- Blackmail attacks possible (M blackmails E)



- General theme of detecting & reacting to misbehavior

- Detect rogue sensors, distribute rating data

The Sybil Attack

- The multiple identities attack

- Relevant in many wired and wireless contexts

- Voting
- Resource allocation
- Trust establishment

- Slides based on presentation by John Douceur

Terminology

- **Entity**
 - Collection of material resources, of specifiable minimal size, under control of a single agency
 - E.g., one desktop computer
- **Identity**
 - Persistent informational abstraction provably associated with a set of communication events
 - E.g., a public key
- **Validation**
 - Determination of identity distinctness
- **Sybil attack**
 - One entity presents multiple identities
 - Defeats redundancy

Sources of Identity Information



- Trustworthy authority



- Yourself
 - implicitly trustworthy
 - not authoritative



- Other entities
 - not necessarily trustworthy
 - not necessarily authoritative

Sources of Identity Information



- Trustworthy authority
 - Certification agency (e.g. VeriSign)
Authority is VeriSign, etc.
 - IP address (used by e.g. CFS)
Authority is ICANN
 - DNS name (used by e.g. SFS)
Authority is ICANN
 - Hardware key (e.g. EMBASSY)
Authority is Wave Systems, etc.

Sources of Identity Information



- Yourself

Determine that two entities are different iff they can perform some task that a single entity can not.

1. Unless unrealistically resource constrained, an entity can present a constant number of multiple identities.
2. All entities must be issued task concurrently; otherwise one entity can present an unbounded number of identities.

Sources of Identity Information



- Other entities

Accept identities that have been validated by a sufficient count of other accepted identities.

1. A sufficiently large set of faulty entities can present an unbounded number of multiple identities.
2. All entities must issue tasks concurrently; otherwise, one entity can present a constant number of multiple identities.

Summary

- Many peer-to-peer systems rely on redundancy
- Redundancy requires establishing distinctness
- With identification authority
 - Explicit (certification agency)
 - Implicit (IP address, DNS name, etc.)
- Without identification authority
 - Nearly uniform resource constraints
 - Simultaneous identity validation
 - Required signatory count exceeds failure count
 - Coordinated identity validation
- Large-scale distributed system requires authority

Project Direction

- Consider Sybil attack in your project
 - Could attacker benefit from multiple identities?
- Can you find a general mechanism to prevent Sybil attack?

The Insecurity of 802.11

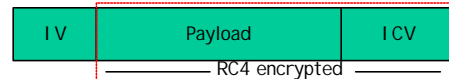
- WEP addresses 802.11 security issues
 - Wired Equivalent Privacy
- Security concerns
 - Wireless offers more opportunities for attack
 - Possible to monitor and participate in a network at a distance (1/2 mi or even further)
- Slides based on Nikita Borisov's Mobicom 2001 presentation

WEP Security Goals

- Prevent link-layer eavesdropping
 - ... not end-to-end security
- Protect message integrity
- Control network access
- Essentially, equivalent to wired access point security
- **None** of these goals are met

Protocol Overview

- Mobile station shares key with access point
- Integrity check value = CRC(payload)
- Payload + ICV are encrypted with the shared key & an initialization vector (IV)
- IV included in the clear
- Receiver decrypts, verifies ICV, and rejects packet if check fails



Encryption Algorithm

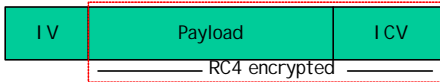
- RC4 – a well-studied algorithm
- RC4 is a stream cipher
- Expands a key into an infinite pseudorandom keystream
- To encrypt, XOR keystream with plaintext
- $Random \oplus Anything = Random$
- Encryption same as decryption

Keystream Reuse

- Using same part of RC4 keystream to encrypt two messages is disastrous:
 - $C1 = P1 \oplus RC4(key)$
 - $C2 = P2 \oplus RC4(key)$
 - $C1 \oplus C2 = P1 \oplus P2$
- Knowledge of P1 reveals P2
- More sophisticated analysis possible based on expected distribution of P1 and P2

Initialization Vectors

- Use initialization vectors to generate different keystream for each packet
- IV augments the shared key:
- $C = P \hat{\Delta} RC4(\text{key}, IV)$
- Different IVs \Rightarrow Different keystreams
- Include IV unencrypted in the packet



IV collisions

- IV collisions – two packets with same IV
 - Therefore same keystream
- 802.11 does not specify how to pick IVs
 - Doesn't even require a new one for each packet!
- Many implementations reset IV to 0 when initialized, increment with each packet
- Easy to find IV collisions!
 - Especially if shared key is used in both directions or by many mobile stations

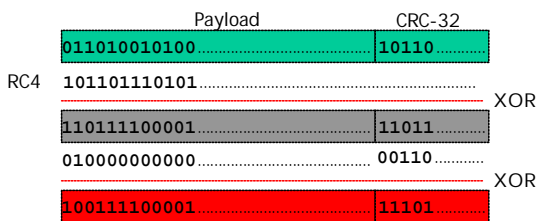
IV collisions, continued

- 24-bit IV – 2^{24} possibilities
- Guaranteed collisions after sufficient time (a few hours to a few days)
- Known plaintext for one packet allows to decrypt any others with the same IV
 - Obtain 2^{24} known plaintexts
 - Store decryption table on a cheap hard drive
 - Several ways to obtain plaintext
- Confidentiality compromised

Problem 2: Linear Checksum

- Encrypted CRC-32 used as integrity check
 - Fine for random errors, but not malicious ones
- CRC is linear
- I.e. $CRC(X \oplus Y) = CRC(X) \oplus CRC(Y)$
- $RC4(k, X \oplus Y) = RC4(k, X) \oplus Y$
- $RC4(k, CRC(X \oplus Y)) = RC4(k, CRC(X)) \oplus CRC(Y)$
 - Hence we can change bits in the packet, without decrypting!

Packet Modification

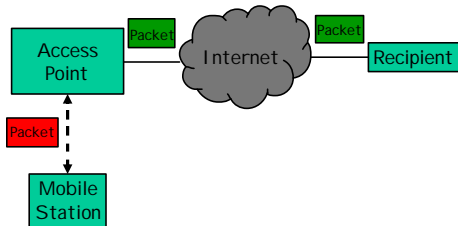


$$RC4(k, CRC(X \hat{\Delta} Y)) = RC4(k, CRC(X)) \hat{\Delta} CRC(Y)$$

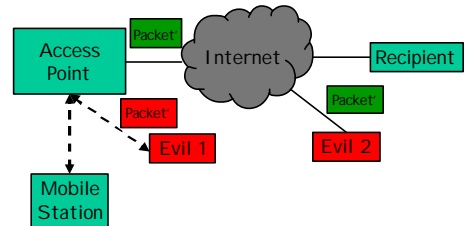
Can modify packets!

- “Integrity check” does not prevent packet modification
- Can maliciously flip bits in packets
 - Modify active streams!
 - Bypass access control
- Partial knowledge of packet is sufficient

Typical Operation



Redirection Attack



Redirection Attack

- Suppose we can guess destination IP in encrypted packet
- Flip bits to change IP to Evil 2, send it to AP
- AP happily forwards it to Evil 2
- Set port to 80 to bypass firewalls

Message Integrity Essential

- Poor integrity checks can lead to compromised confidentiality
 - Redirection attack
 - TCP reaction attack
 - Use TCP checksum to recover plaintext
 - Inductive CRC attack ([Arbaugh'01])
- Rule of thumb: whenever you encrypt, also use a MAC

Attack Practicality

- Sit outside competitor's office, use a software radio
- ... or an off the shelf wireless card!
- With minimal work, possible to monitor encrypted traffic
 - Commercial sniffers also available
- More work to mount active attacks
- But it only has to be done once
 - Scripts can be distributed by underground channels

Lessons

- Security hard to achieve
 - Even when good crypto is used
- Conflicting design objectives
 - E.g. "be liberal in what you accept"
- Public review is a Good Idea
 - Time to develop attacks is short!
 - Update: 802 standards are now freely available
- Use previous work (and their failures)
 - Similar attacks on other systems (e.g. earlier versions of IPSEC) have been shown