Adversary Models

CPEN 442 "Introduction to Computer Security"

Konstantin Beznosov

why we need adversary models?

- attacks and countermeasures are meaningless without

elements of an adversary model

- objectives
  - obtain secret(s): decrypt cipher-text, guess/find password
  - obtain access to assets: access to an account, full or partial control of a system or its parts
- initial capabilities
  - knowledge of (1) keys, passwords, and other secrets, (2) system/ environment design/architecture
  - access to the system's source code and other implementation details
  - partial access to a system (PC, server, mobile device)
  - partial control of a system (direct browser to a URL, control of a low-privilege account)
- capabilities during the attack
  - passive: eavesdropping messages
  - active: modifying, re-playing, or removing messages
  - running code on the target system
  - observing system at run-time

Dolev-Yao model

- the network is completely under the adversarial control
  - can record, delete, replay, reroute, reorder, and completely control the scheduling of messages.
- the adversary is the network
  - the honest participants send their messages only to the adversary and receive messages only from the adversary.
- the adversary can choose the recipient and auxiliary information for its messages with total non-determinism
- initial knowledge of the adversary
  - the public keys (K_{Pub}),
  - the private keys of subverted participants ($K_{Adv} \subseteq K_{Priv}$),
  - the identifiers of the principals (I), and
  - the nonces the adversary itself generates ($R_{Adv} \subseteq R$), which are assumed to be distinct from all nonces generated by honest participants.

Dolev-Yao model (continued)

- message M is derivable by adversary from a set of messages S, if it's possible to produce by applying the following operations a finite number of times:
  - decryption with known or learned private keys
  - encryption with public keys
  - pairing of two known elements
  - separation of a pair into its components

Chip & PIN

EMV protocol

Europay, MasterCard, VISA (EMV) -- protocol for payment cards with chips (and PINs)

750M cards currently deployed

a three phase protocol:

- Card authentication
  - type of card, issuer, verification method list etc)
- Cardholder verification, based on verification method list,
  - PIN
  - signature
  - nothing
- Transaction authorization
  - card generates secured transaction info for the issuing bank clearance

a complete run of a Chip & PIN protocol

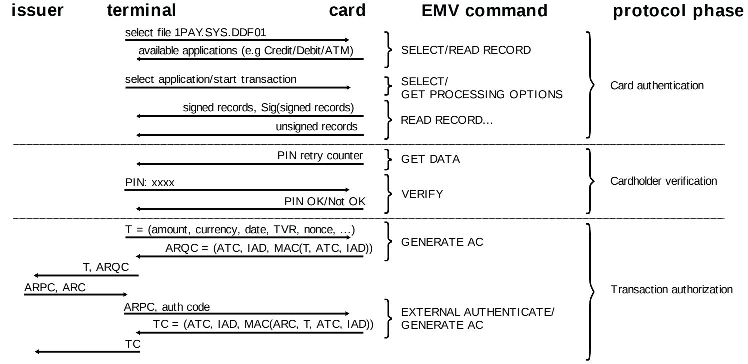


Figure 2. A complete run of a Chip and PIN protocol.

adopted from [1]

video clip

http://www.youtube.com/watch?v=JPAX32lgkrw

cardholder verification step

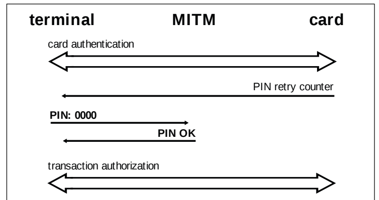


Figure 3. The man-in-the-middle suppresses the PIN Verify command to the card, and tells the terminal that the PIN has been verified correctly. A complete transaction is detailed in Appendix A.

adopted from [1]

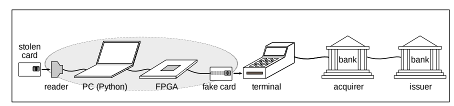
- attacker tricks the card into “thinking” it’s doing a chip-and-signature transaction while the terminal “thinks” it’s chip-and-PIN.

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

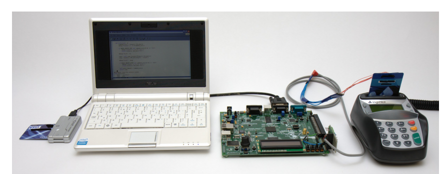
adopted from [1]

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

the attack



adopted from [1]



adopted from [1]

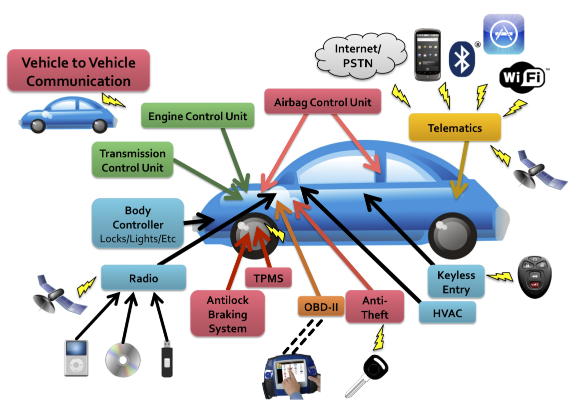
a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

adversary model

- objectives
  - pay to a street merchant with a stolen payment C&P card
- initial capabilities
  - can still payment C&P cards
  - can purchase or make necessary equipment for the MITM attack
- capabilities during the attack
  - conceal the equipment from the merchant's staff
  - conceal the fact that the fake card has wires attached to it
  - insert the fake card in the merchant's terminal

Security Analysis of a Modern Car

today cars



adopted from [2]

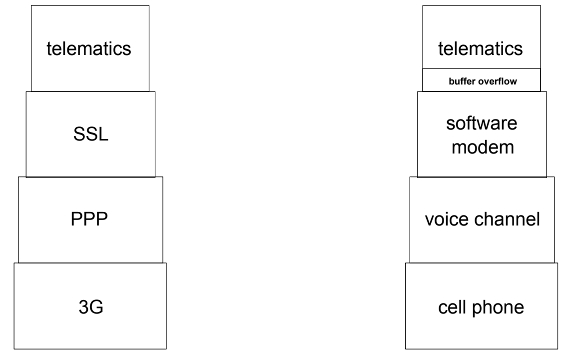
indirect physical access: media player attack

- attack 1: vestigial radio reflash from CD code
- attack 2: WMA parsing bug -> buffer overflow
- on-radio debugger
- insert CD containing malicious WMA file
- compromise the car

short-range wireless: Bluetooth attack

- common embedded Bluetooth stack on telematics unit
  - strcpy() bug
- Android trojan compromises telematics ECU
- can undetectably pair a bluetooth device
  - USRP-based software radio
  - brute force PIN
  - cannot be unpaired with standard interface

long-range wireless: cellular attack



- call telematics unit
- transmit malicious payload (using modem protocol or just play malicious sound track over phone)

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA
ece Ele Cor Eng

what's next?

- remotely trigger code from prior compromise
  - proximity trigger
  - broadcast trigger (FM RDS)
  - short-range targeted trigger (Bluetooth)
  - global targeted trigger (cellular)

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA
ece Ele Cor Eng

what can an adversary do with this?

- car theft
  - compromise car
  - locate it via GPS
  - unlock doors
  - start engine
  - bypass anti-theft
  - video demo: http://www.youtube.com/watch?v=bHfOzilwXic (minute #16)
- surveillance
  - compromise car
  - continuously report GPS coordinates
  - stream audio recorded from the in-cabin mic

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA
ece Ele Cor Eng

adversary model

- objectives
  - take control over parts or the whole car in order to perform surveillance, theft, or cause car accident.
- initial capabilities
  - access to equipment and documentation to develop and test an attack
    - extract device's firmware
    - reverse engineer firmware
    - identify and test vulnerable code paths
    - weaponize exploits
- capabilities during the attack (one of the three)
  - indirect physical access to the car
    - interacts with a physical object that interacts with the car
      - diagnostic tool that plugs directly into OBD-II port
      - entertainment systems (CD player, digital multimedia port, iPod Out)
  - short-range wireless signals (between 5 and 300 meters)
    - Bluetooth, Remote Key Entry, RFID car keys, Tire Pressure Monitoring Systems, WiFi, Dedicated Short Range Communications
  - long-range wireless signals (greater than 1 km)
    - broadcast channels: GPS, satellite radio, digital radio, Radio Data System, Traffic Message Channel

summary: adversary model

- objectives
- initial capabilities
- capabilities during the attack

references

1. Chip and PIN is Broken, Murdoch, Steven J.; Drimer, Saar; Anderson, Ross; Bond, Mike; , "Chip and PIN is Broken," 2010 IEEE Symposium on Security and Privacy (SP), pp.433-446, 16-19 May 2010, doi: 10.1109/SP.2010.33
2. "Comprehensive Experimental Analyses of Automotive Attack Surfaces," S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, USENIX Security, August 10–12, 2011.