Introduction to Information Security
14-741/18-631 Fall 2021
Unit 1: Lecture 2: Threat Model

Limin Jia liminjia@andrew

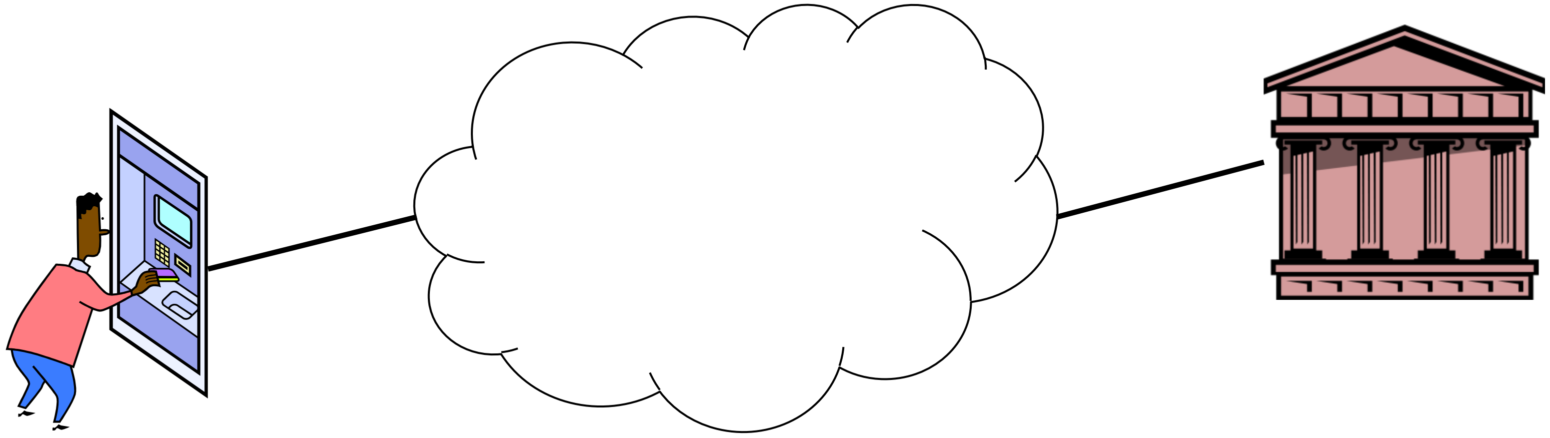
Threat model of Japanese puzzle box

Threat model of Japanese puzzle box

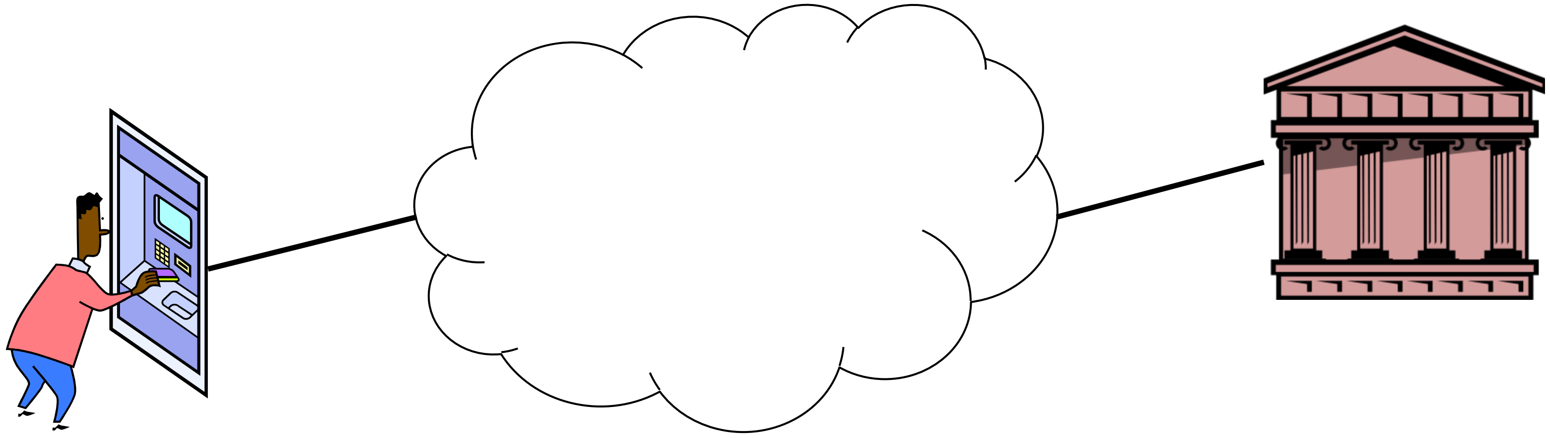
This lecture's agenda

- **Why Cryptosystems Fail**
- **Attack trees: “listing failure modes”**
- **STRIDE: classifying types of attacks**
- **Objectives of the lecture**
  - Get an understanding of possible failure modes in information systems and associated threat models
  - Expose you to concrete examples of technique for preliminary system security analysis

Analyzing the security of ATM



Analyzing the security of ATM

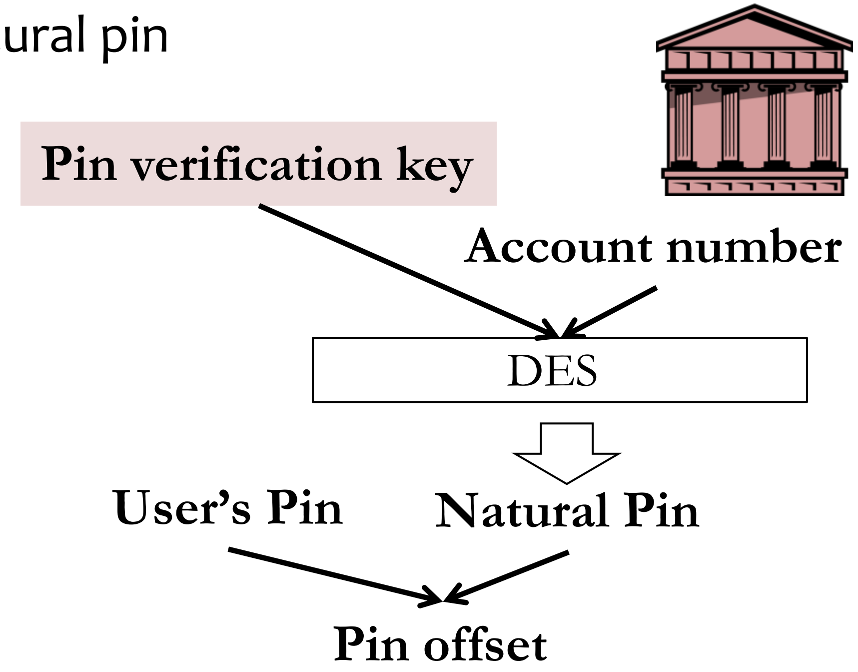


The software/hardware
Employees at the bank
Postmen deliver the card/pin to customers

How does ATM verify pins?

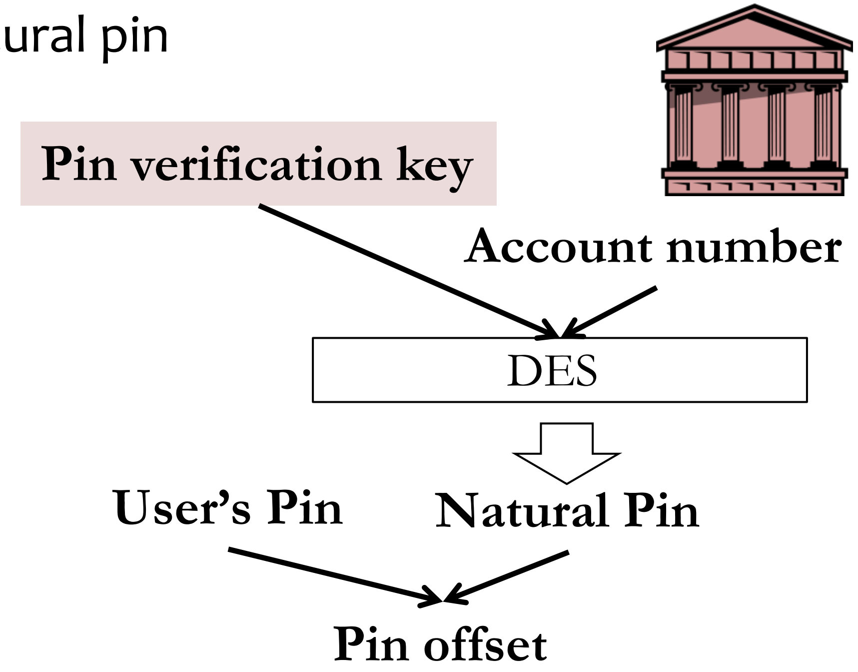
No need to remember the details, just an example complex system for discussion.

- **Create PIN:**
  - PIN verification key to derive a natural PIN from an acct number
    - DES: a mathematical transformation process
  - The user’s selected pin combined with the natural pin to derive pin offset
  - Only Pin offset is stored
  - Without the pin verification key, attacker can’t know the natural pin



How does ATM verify pins?

- **Create PIN:**
  - PIN verification key to derive a natural PIN from an acct number
    - DES: a mathematical transformation process
  - The user's selected pin combined with the natural pin to derive pin offset
  - Only Pin offset is stored
  - Without the pin verification key, attacker can't know the natural pin
- **Verify PIN:**
  - Re-compute Pin offset using acct number and user's pin
  - Compare it with the stored one



How does ATM verify pins?

- ATM is connected via a network

Pin verification key

Account number

DES

Account number

User's Pin

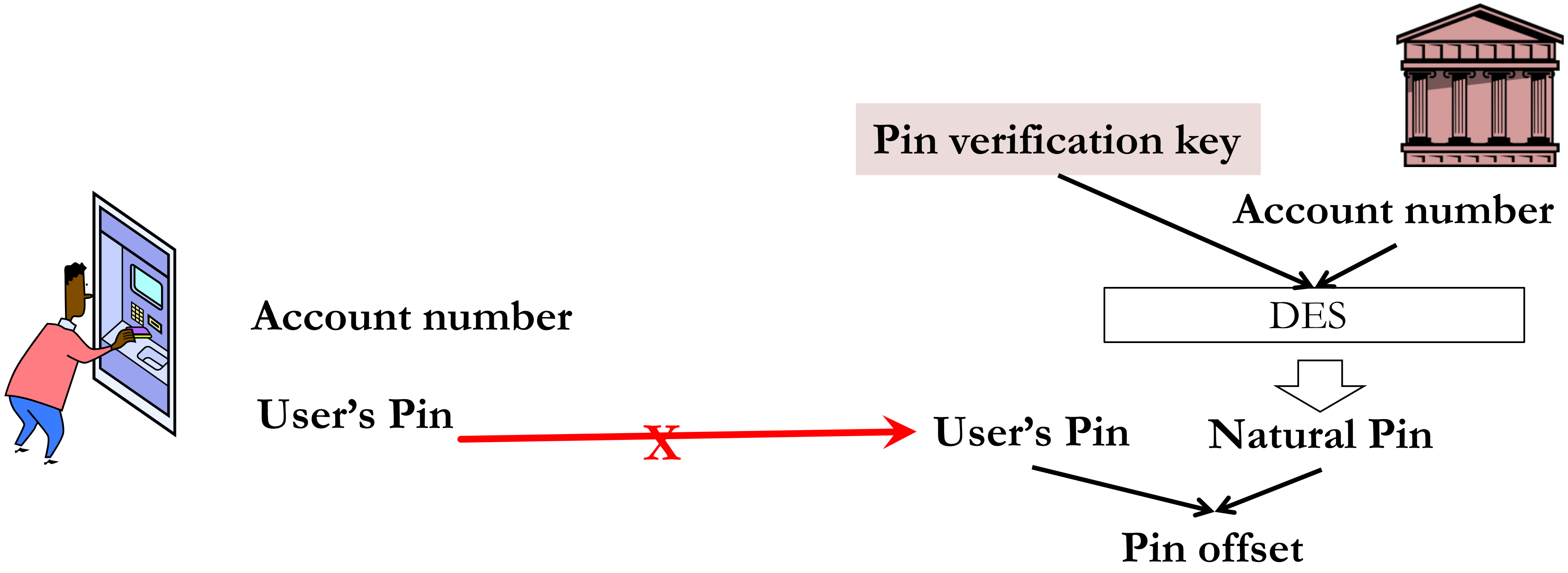
User's Pin

Natural Pin

Pin offset

How does ATM verify pins?

- ATM is connected via a network
- Can’t send pin in the plain to the bank



How does ATM verify pins?

- ATM is connected via a network
- Can’t send pin in the plain to the bank

Enc(Pin enc key, pin)

Pin encryption key

Account number

User’s Pin

Enc(Pin enc key, pin)

Pin verification key

Account number

DES

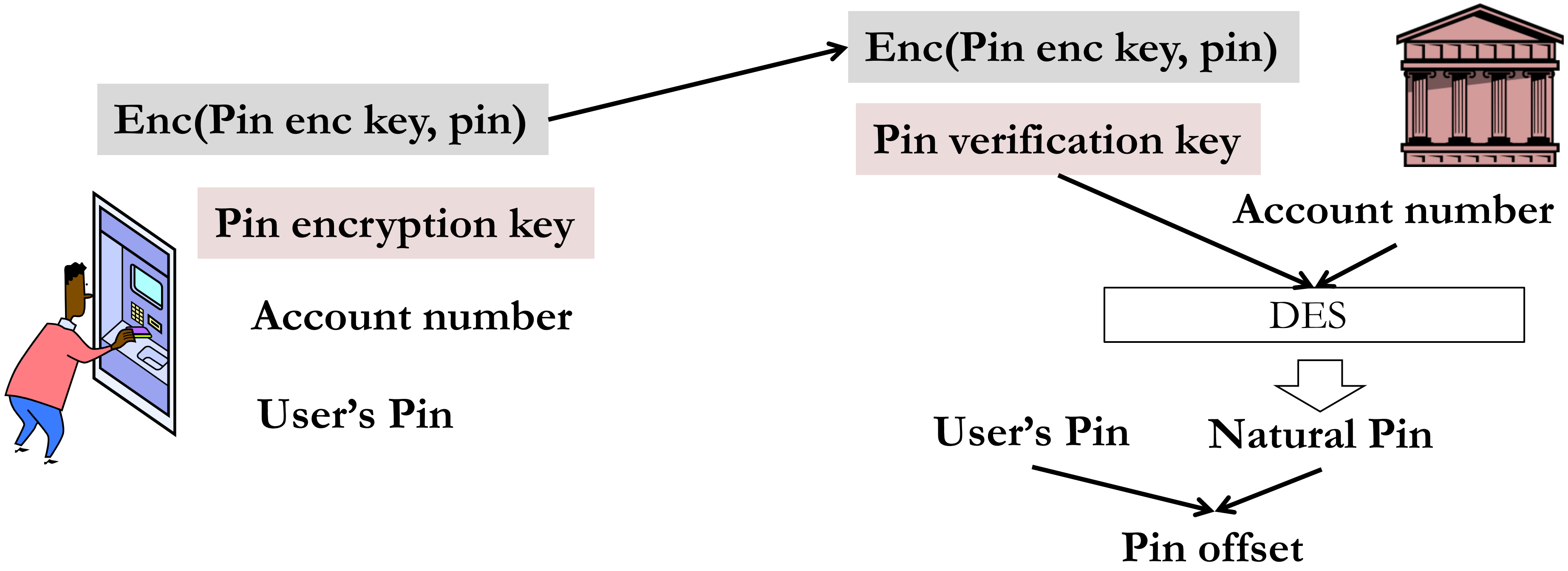
User’s Pin

Natural Pin

Pin offset

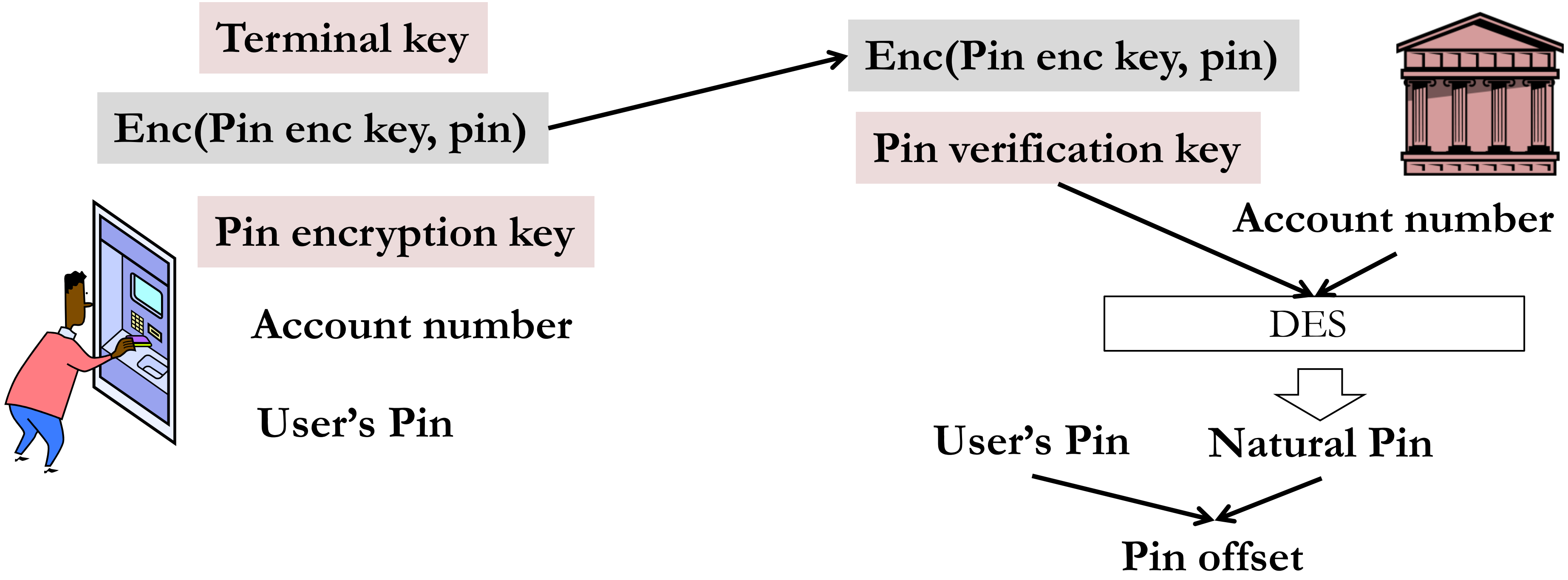
How does ATM verify pins?

- ATM is connected via a network
- Can’t send pin in the plain to the bank
- Encrypt pin using pin encryption key
- How does ATM get pin encryption key?



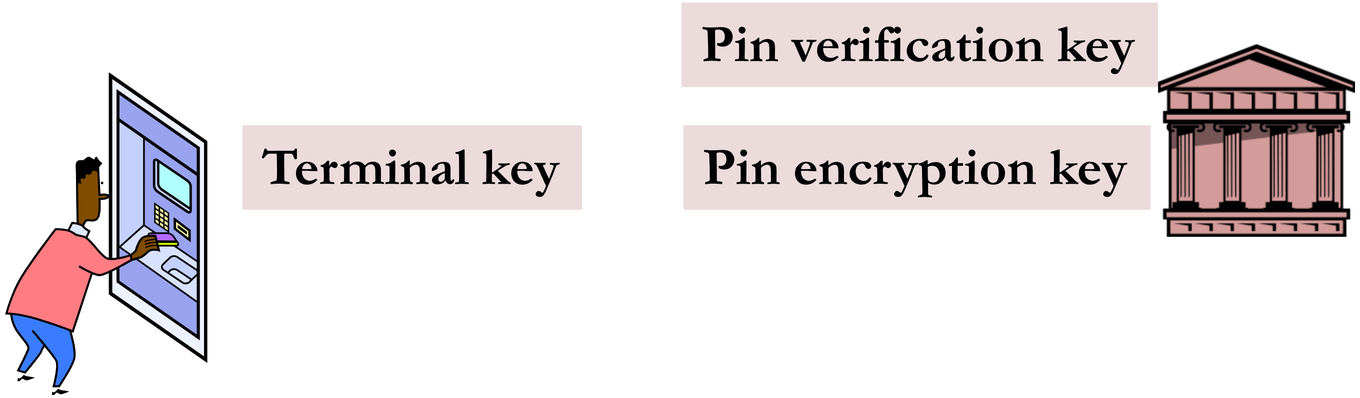
How does ATM verify pins?

- ATM is connected via a network
- Can’t send pin in the plain to the bank
- Encrypt pin using pin encryption key
- How does ATM get pin encryption key?

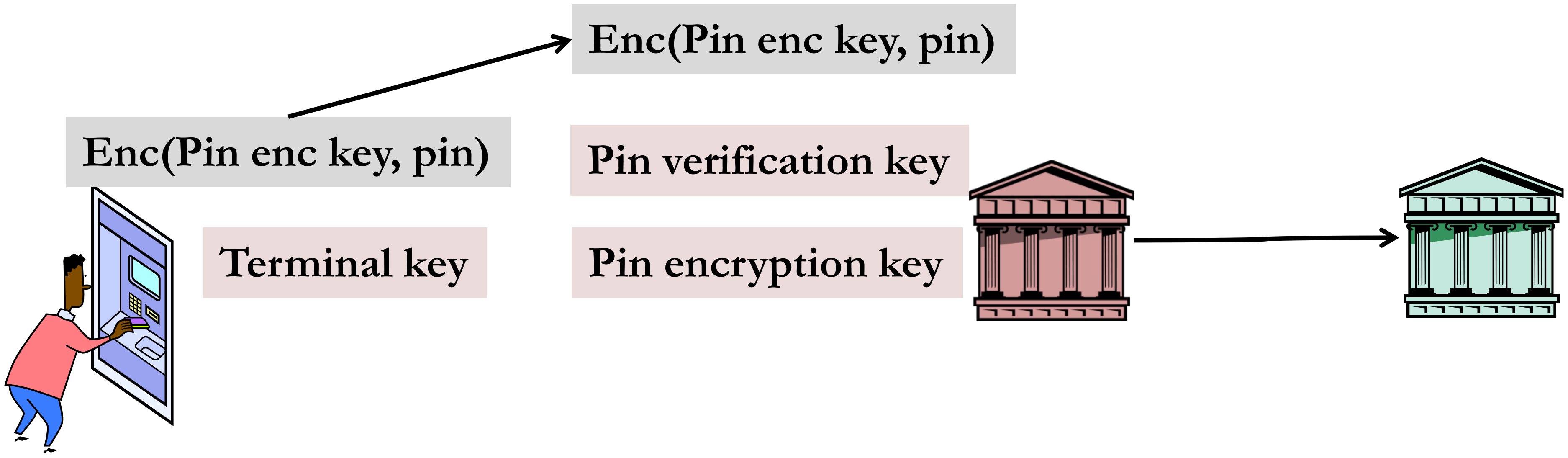


How does ATM verify pins?

- **PIN verification key to derive a PIN from an acct number**
- **PIN encryption key to encrypt a PIN at ATM**
- **Terminal key so that the central bank can transmit the PIN encryption key encrypted**
  - Terminal key is physically installed by bank employees

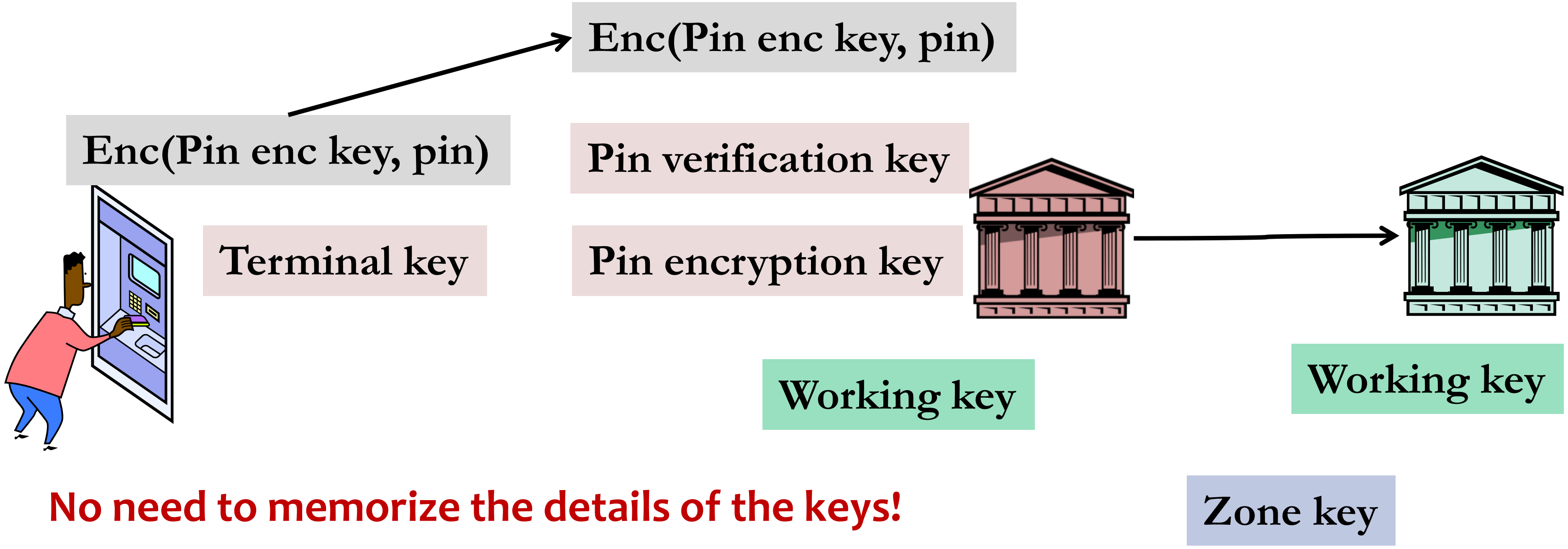


How does ATM verify foreign pins?



How does ATM verify foreign pins?

- Working keys to allow transactions with foreign banks
- Zone keys to allow encrypted transmissions of working keys



No need to memorize the details of the keys!

Why cryptosystems fail

- **Seminal paper by Ross Anderson from 1993**
- **Back in 1990s**
  - Security = cryptography
  - Almost all cryptographers work for NSA
  - As late as 1992, cryptography was on the U.S. Munitions List as an Auxiliary Military Technology
  - Security by obscurity doesn't sound that bad

Why cryptosystems fail

- **Seminal paper by Ross Anderson from 1993**
- **Draws analogy between information security and airline industry**
  - Airlines: low risk because failures are highly publicized and analyzed
  - Information security: generally security by obscurity
    - Government classification, proprietary protocols
    - We don’t learn from our mistakes
- **Makes the case that information security must become much more open to investigation**
  - Example: ATM fraud in the UK

Policy differences between countries

- **In the U.S.**
  - In case of theft, customer bears almost no responsibility on the charges incurred
- **In the U.K. (and in many other countries)**
  - Customer has to bear risk!
  - No incentive for the bank to be overly concerned about security (at the time the paper was written)
  - Many “phantom withdrawals”

Insider attacks

- **Banker's ability to issue a 2nd card**
  - Could even conceal withdrawals in some cases
- **Technical staff can tamper with the ATM**
- **Policy breakdowns**
  - Some manager decides to remove most security primitives to save costs
  - Manager is powerful, no one complains, fraud increases

Outsider attacks

- **Postal interception of cards and PINs**
- **Replay attacks**
  - ATM is bugged with a recording device
  - Authorization to pay is recorded, and then replayed at will
  - “Jackpotting” (popular in the 80’s)
- **Test transactions**
- **False terminals**

Fake slot

Wireless camera

Guessable PINs

- **Generally, PINs should be 4-digits taken from the encrypted version of the bank account**
  - 10,000 possibilities if truly random
- **Most ATMs allow for 3 trials**
  - 1 chance in 3,333 that a crook guesses the right PIN before card is swallowed by ATM
- **Unfortunately, some banks use:**
  - Constraints on PINs to make them easier to verify by weak POS that don't have encryption
    - E.g., $d1+d4 = d2+d3$ → 1,000 possible combinations
  - Visual aids → about 20-30 possible combinations
  - Personally chosen PINs
    - Can be easily guessable
    - Identification by bank clerks
  - PINs selected by the bank (has no relation to the accnt no.) and encrypted on card itself!

Complex fraud

- **Protecting keys requires**
  - No single entity knows a full key
  - Keys are not physically accessible
  - Security module (PC in a safe)
- **Often defeated in practice**
  - Software encryption instead of security module
  - Maintenance engineers get full access to a terminal key
  - Trapdoors (physical or logical)
  - Shared PIN keys(!) among institutions
  - Weakly encrypted keys
    - Poor encryption algorithms (pre-DES)
    - Poor encryption parameter selection (e.g., not enough bits)

Lessons learned

- **Security by obscurity**
  - No prior experience available
- **Result: Threat model was wrong**
- **Focused on what could possibly go wrong**
  - Relatively complex key system to ensure secrecy
- **Should have focused on what was likely to go wrong**
  - Human error rendering cryptosystem useless
  - Should consider both human and tech. factors

Recommendations

- Get inspiration from safety-critical systems
- List all possible failure modes
- Document which strategy is used to make each failure mode impossible
- Review the proposed implementation of strategies by many experts
- Certification required to ensure properly trained personnel is in charge of maintenance of cryptosystem

Possible strategies

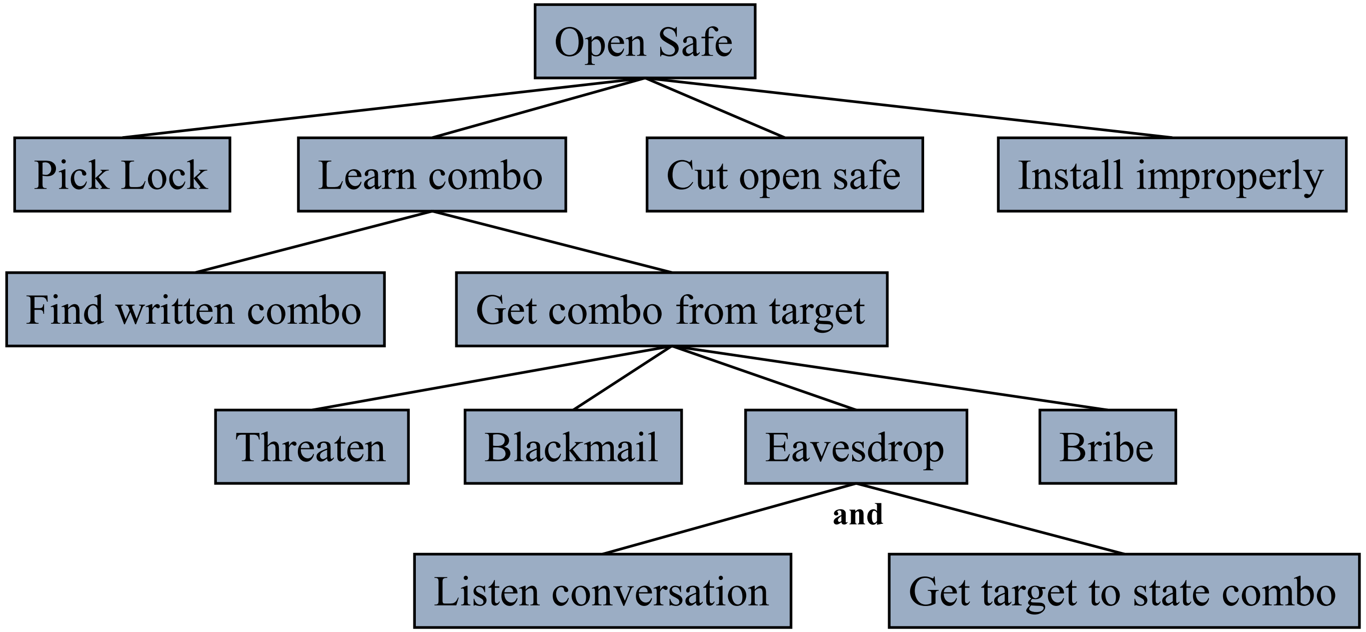
- **Formal verification**
  - Similar to railway system
  - Used in cryptology
- **Feedback loop failure analysis and design guidelines**
  - Similar to avionics
  - E.g., wireless security: WEP → 802.11i
- **More reading**
  - Chip and pin
  - http://www.cl.cam.ac.uk/research/security/banking/

Did we learn the lessons?

- **EMV: Why Payment Systems Fail**
  - 24 years later – same author (Ross Anderson, adding Steven J. Murdoch)
- **Chip and pin/signature cards**
  - Yes cards: copy chip certificate and say “yes” to any PIN
  - Can defeat with online transaction verification (requires chip to verify transaction details) or Dynamic Data Authentication (requires crypto processor in chip)
  - Side-effect: PIN use in stores made it easier to create magnetic strip cards and steal from ATMs

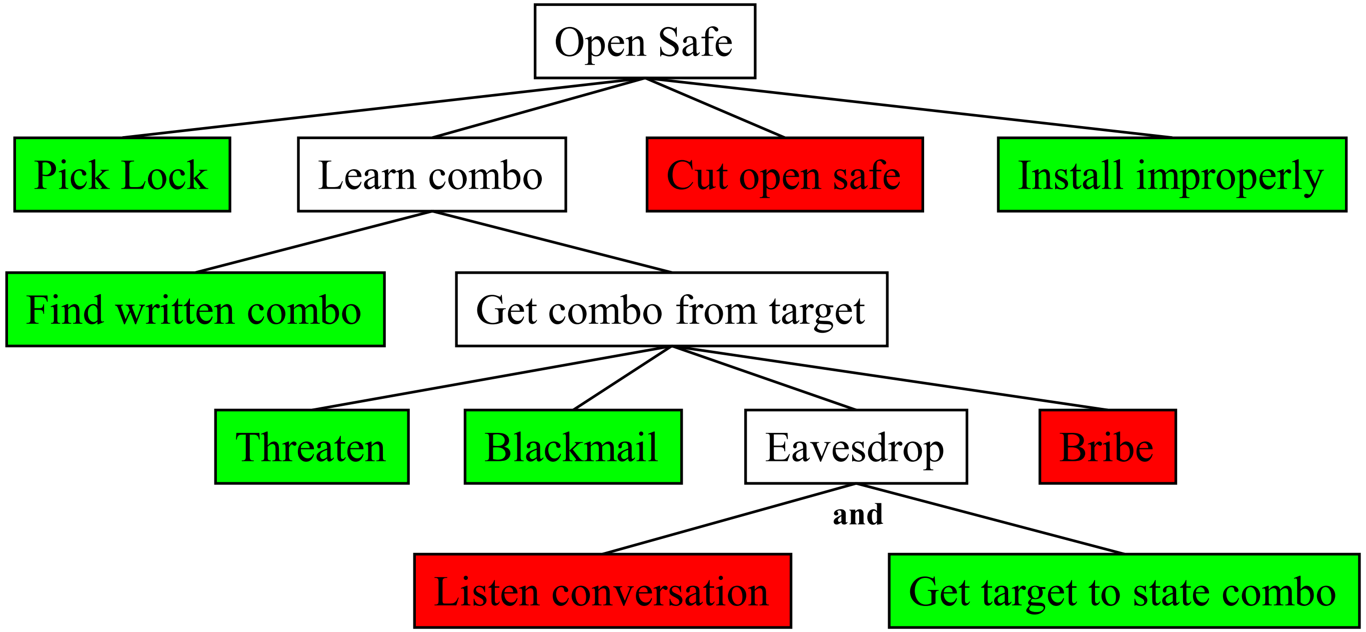
Boolean attack tree (Schneier)

- Listing all possible failure modes
- Example: safe (incomplete)



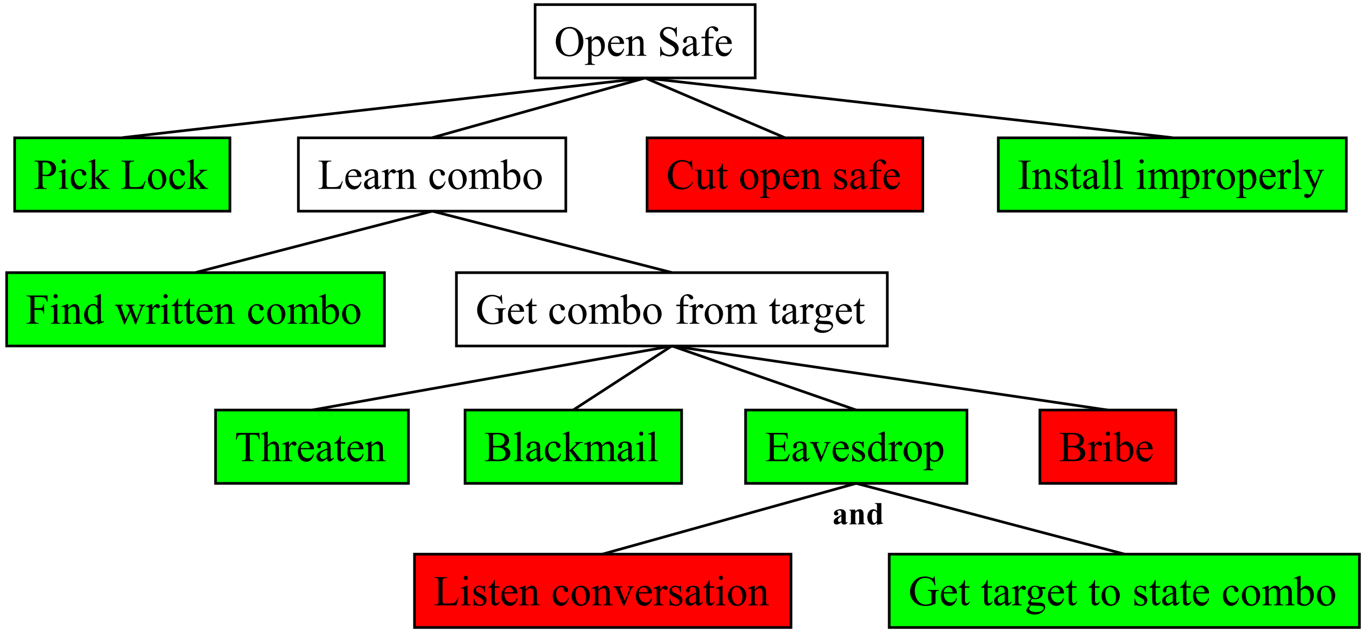
Boolean attack tree

- **Listing all possible failure modes**
- **Example: safe (incomplete)**



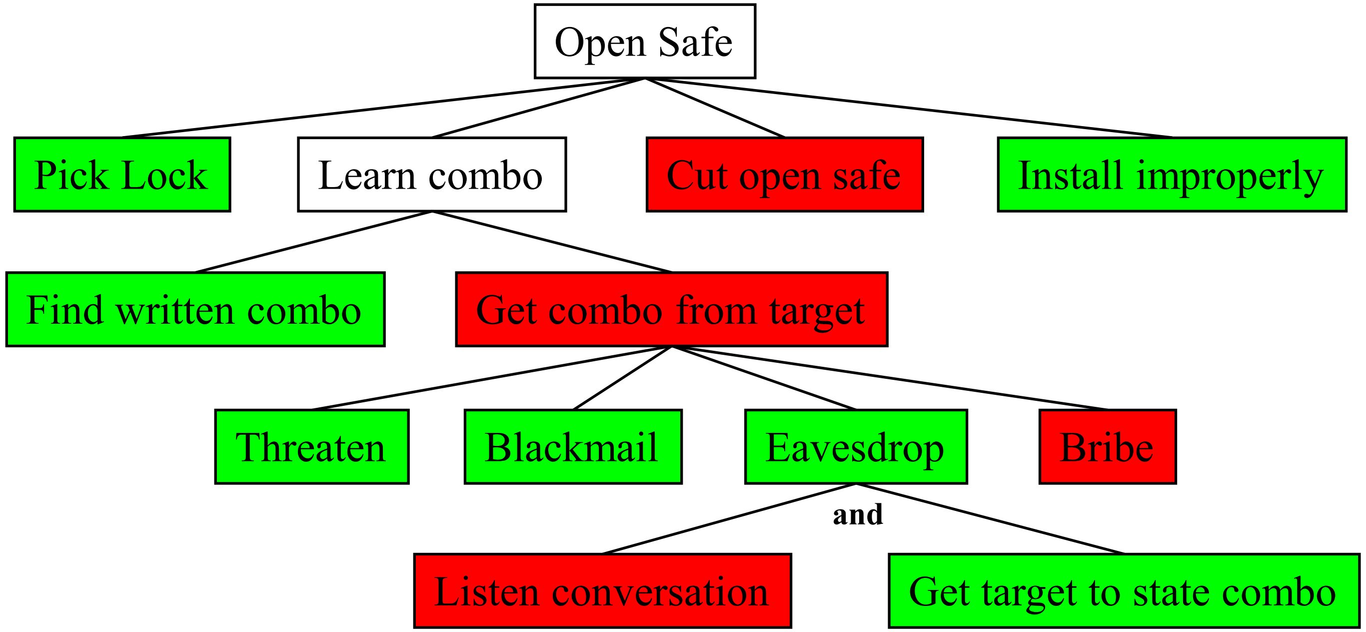
Boolean attack tree

- Listing all possible failure modes
- Example: safe (incomplete)



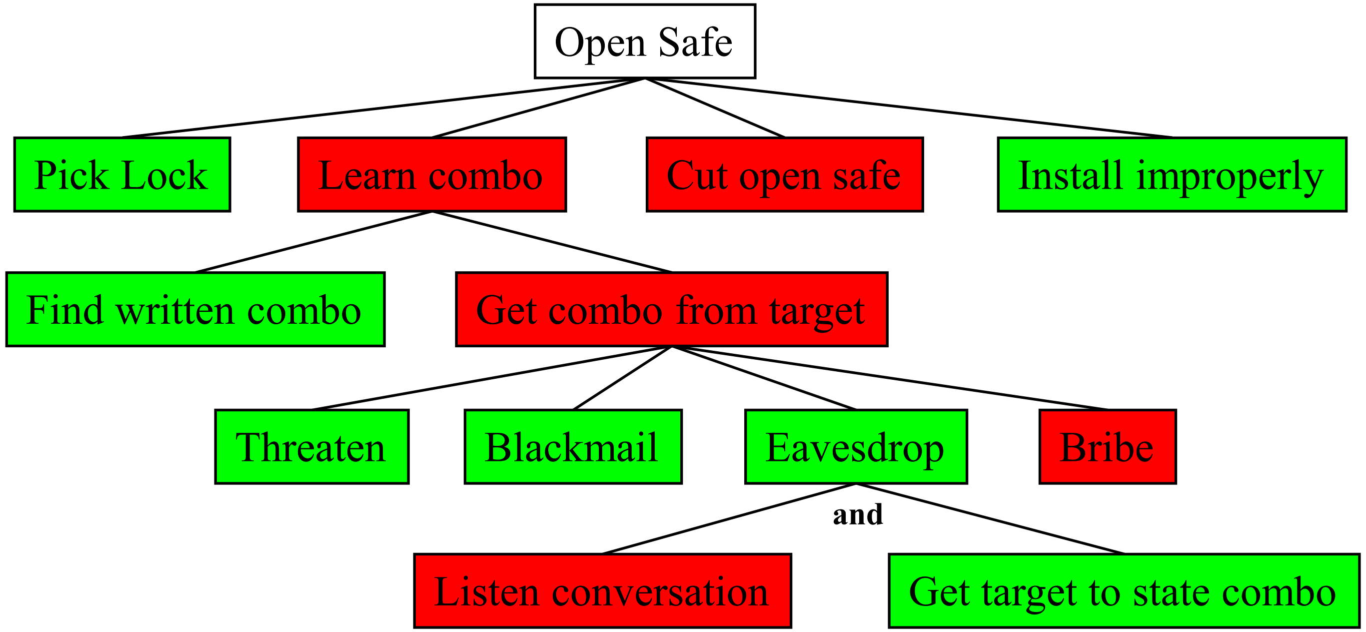
Boolean attack tree

- Listing all possible failure modes
- Example: safe (incomplete)



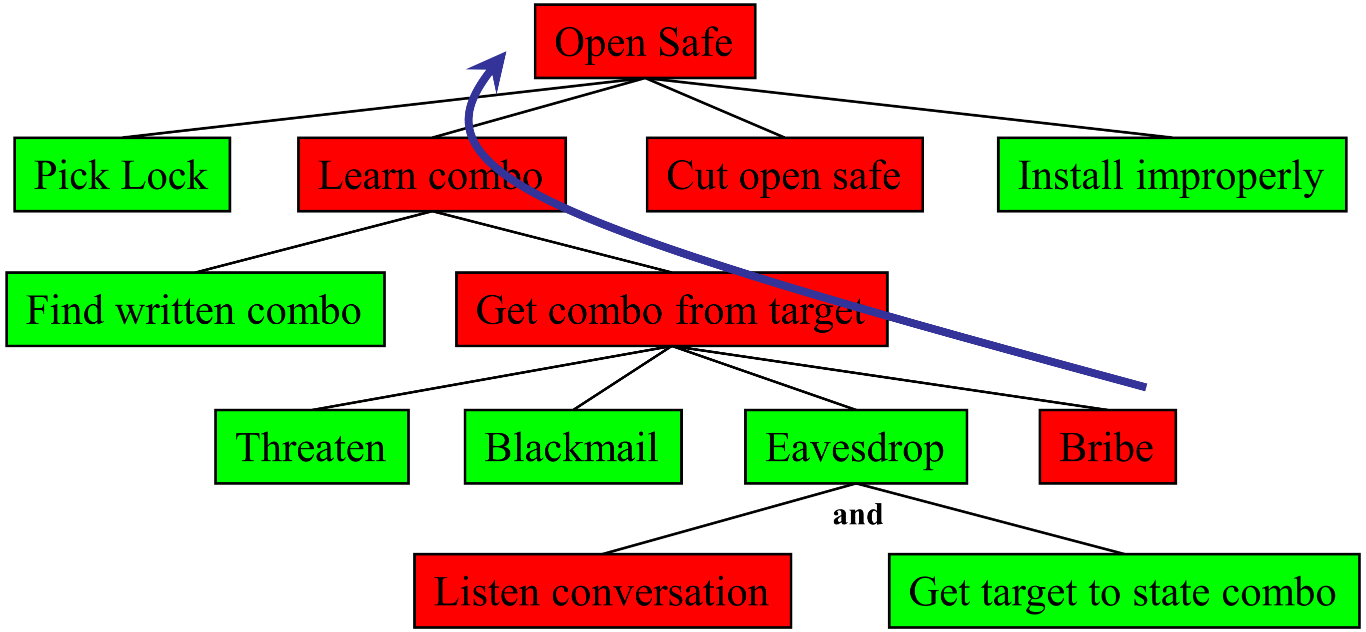
Boolean attack tree

- Listing all possible failure modes
- Example: safe (incomplete)



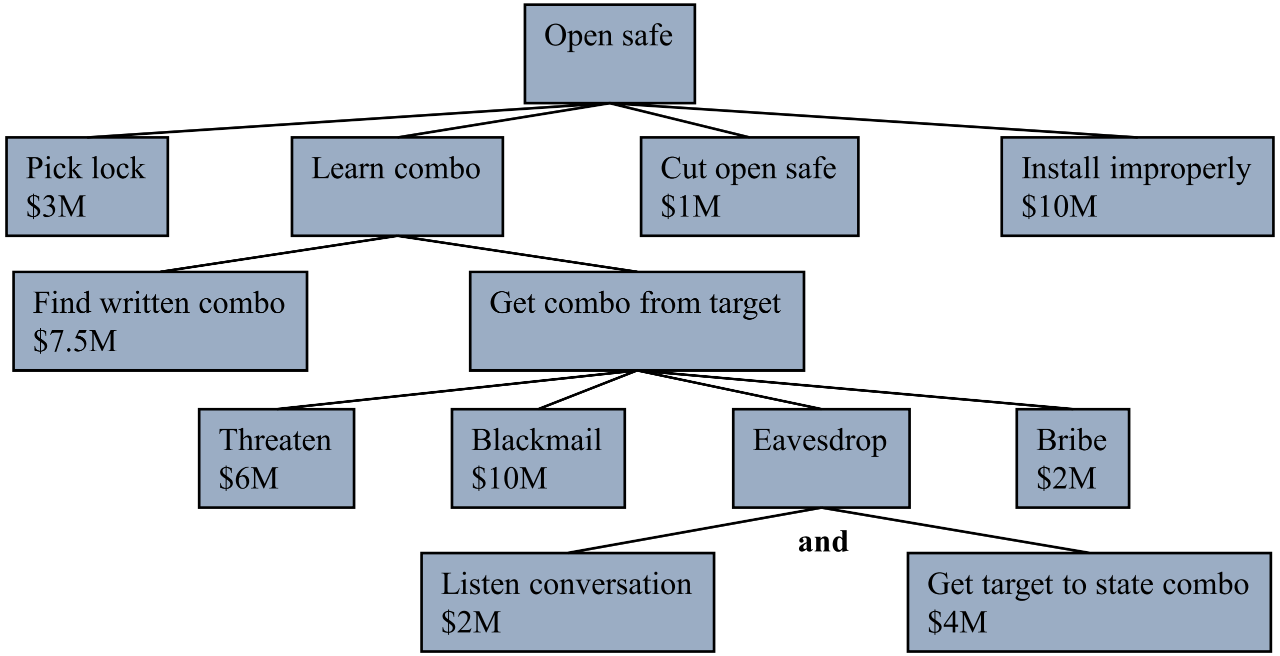
Boolean attack tree

- **Listing all possible failure modes**
- **Example: safe (incomplete)**



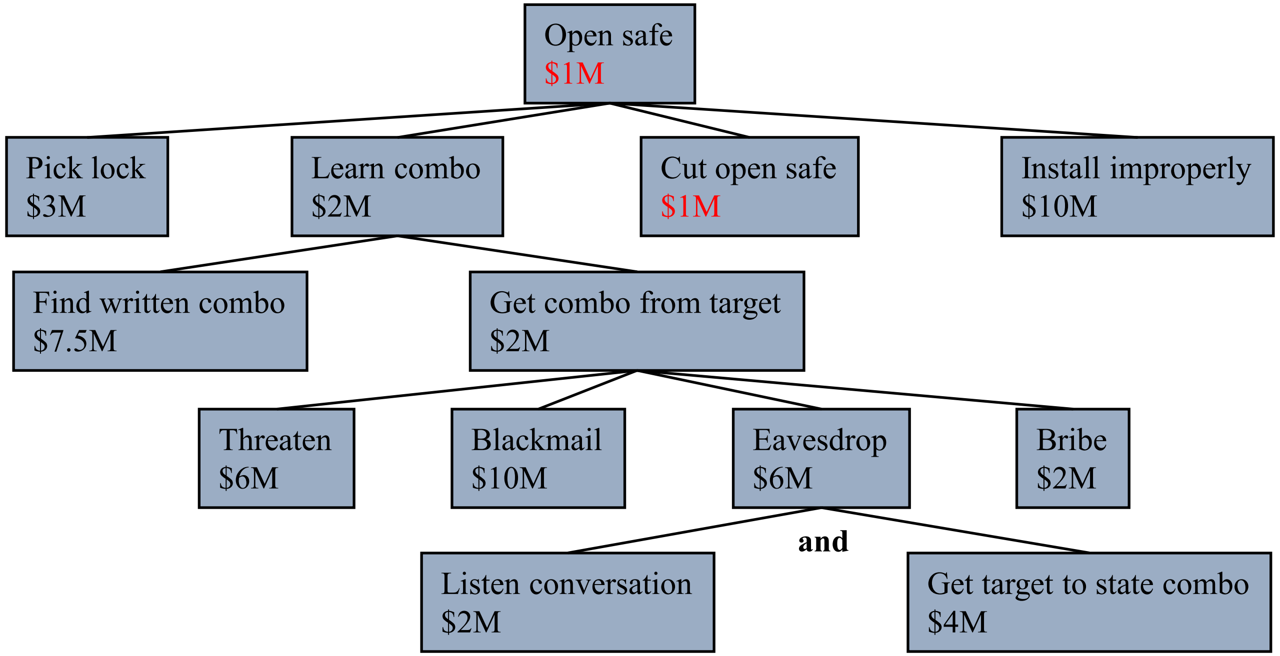
Parameterized attack tree

- Can be used to assess the cost of an attack
- Can use other quantities (e.g., probabilities) instead



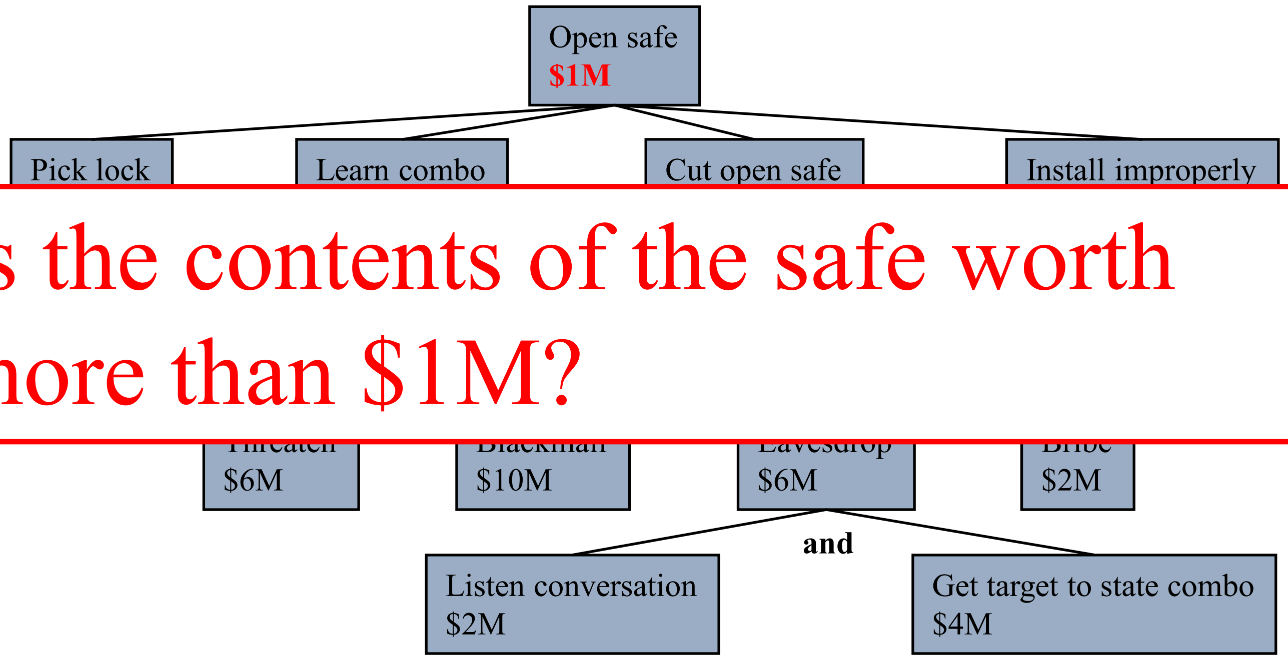
Parameterized attack tree

- Can be used to assess the cost of an attack
- Can use other quantities (e.g., probabilities) instead



Parameterized attack tree

- Can be used to assess the cost of an attack
- Can use other quantities (e.g., probabilities) instead



Is the contents of the safe worth more than $1M?

Practical attack trees

- **Generally multi-parameter**
  - Probabilities
  - Monetary cost
- **Combination of continuous and boolean parameters**
  - Requires special equipment/knowledge…

- **Needs to be correlated with knowledge about attackers to be useful**

STRIDE

- **Threat model by Microsoft**
  - https://www.owasp.org/index.php/Threat_Risk_Modeling#STRIDE
- **Six categories**
  - Spoofing of user identity
  - Tampering
  - Repudiation
  - Information disclosure (privacy breach or data leak)
  - Denial of service (D.o.S)
  - Elevation of privilege

STRIDE

- Draw a picture of the system
- Anywhere you see communication, this is a trust boundary where you should do analysis!

STRIDE

- **CMU Directory Service (https://directory.andrew.cmu.edu/)**
  - Anybody can query faculty and staff by name
  - CMU person can query student by name
  - Only admins can modify entries
- **What are the threats you can envision?**
  - Spoofing of user identity
  - Tampering
  - Repudiation
  - Information disclosure
    (privacy breach or data leak)
  - Denial of service (D.o.S)
  - Elevation of privilege

Take away

- **Security is about**
  - Ensuring a system works as intended in face of potentially malicious adversaries
  - Risk management, threat management
- **Security can be achieved by**
  - legal, social, economic, or technological means
  - most likely by a combination of all of the above
- **No security by obscurity!**
  - Kerckhoff's principle: "a cryptosystem should be secure even if everything about the system, except the key, is public knowledge"
- **Instead:**
  - Inspiration from safety-critical systems
  - Understand the system and attacks
  - Openness, public review, proper training and certifications
  - Combination of formal verification and feedback-loop design and analysis
  - Design for defense and recovery
  - Attack trees: a practical way of listing all the vulnerabilities of your system
  - Benefit from incremental improvements (feedback)