Is “Wireless Security” an Oxymoron?

Bruce McNair

Stevens Institute of Technology
bmcnair@stevens.edu
http://www.ece.stevens-tech.edu/~bmcnair/

Novidesic Communications, LLC
bmcnair@novidesic.com
http://www.novidesic.com

Outline

- Definition of Security
- Security Architecture
- Case examples in wireless **in**security
- Background on cryptography, as related to a case example
- Observations
- Implications
- Security Assessment
- Lessons
- Conclusions
- Future research directions

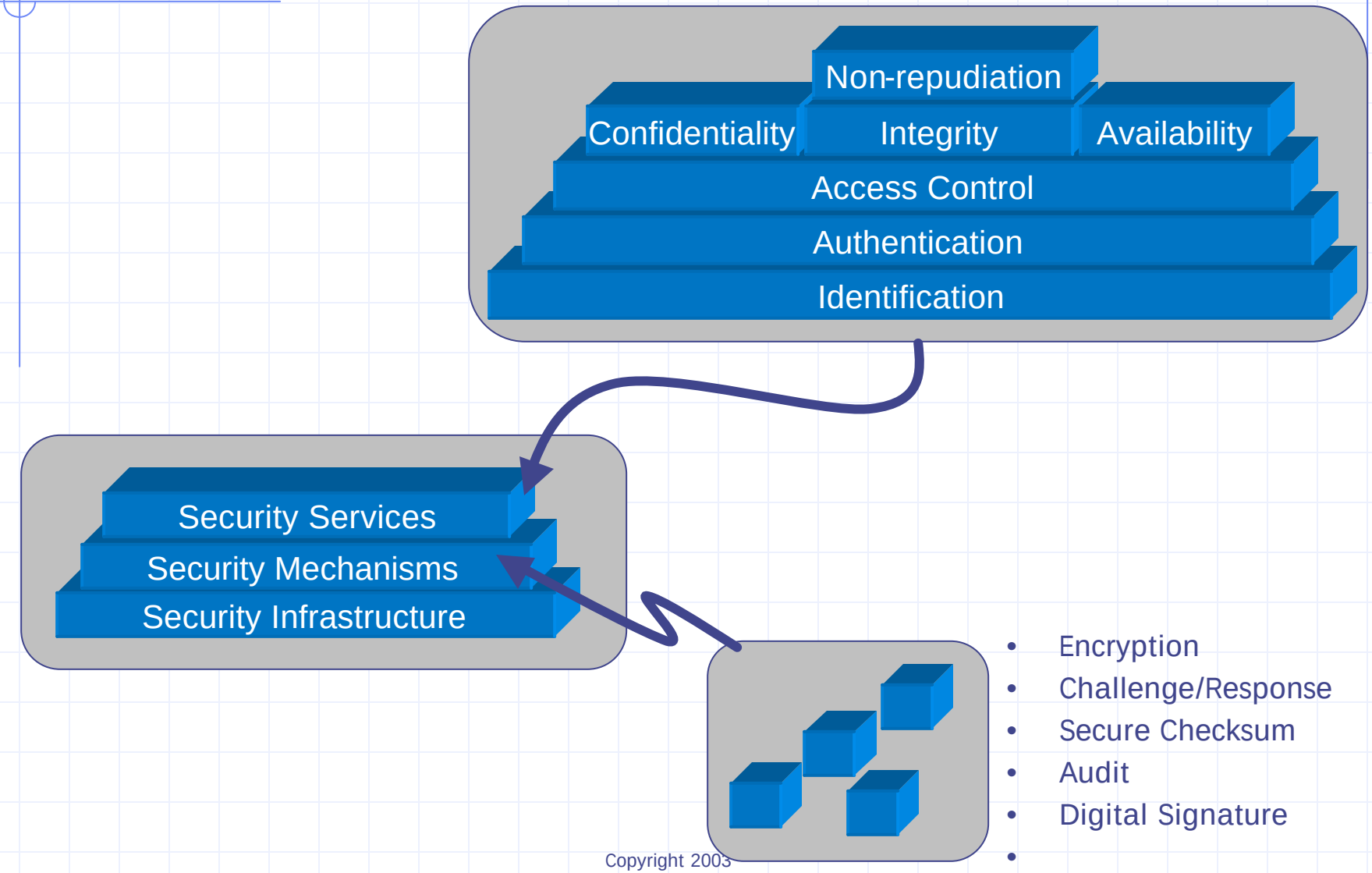
Definition of Security

- Quality: “Meeting or exceeding customers’ expectations”

Definition of Security

- Quality: “Meeting or exceeding customers’ expectations”
- Security: “Meeting or exceeding customers’ expectations *in the presence of the actions of an adversary* ”

Security Architecture

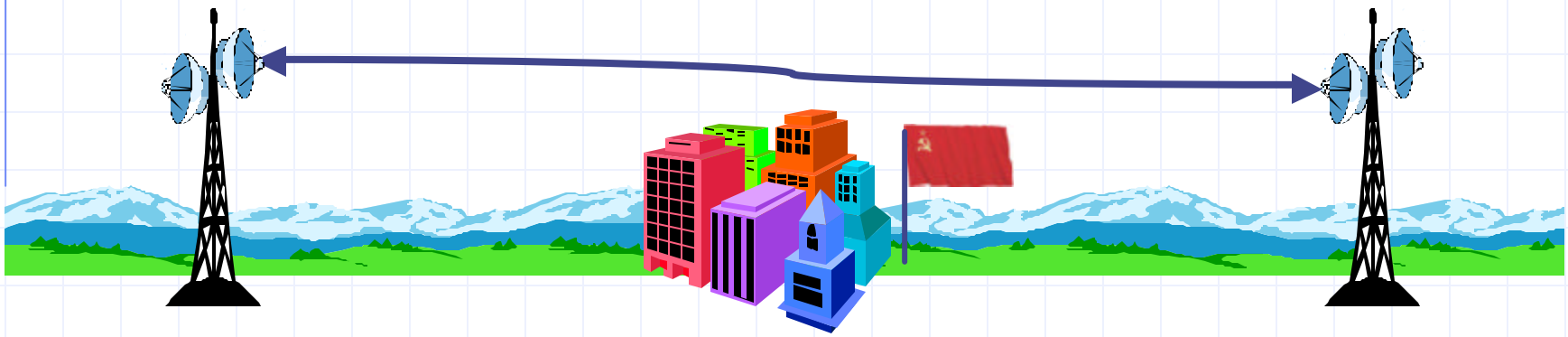


- Encryption
- Challenge/Response
- Secure Checksum
- Audit
- Digital Signature
-

Examples of Wireless Insecurities

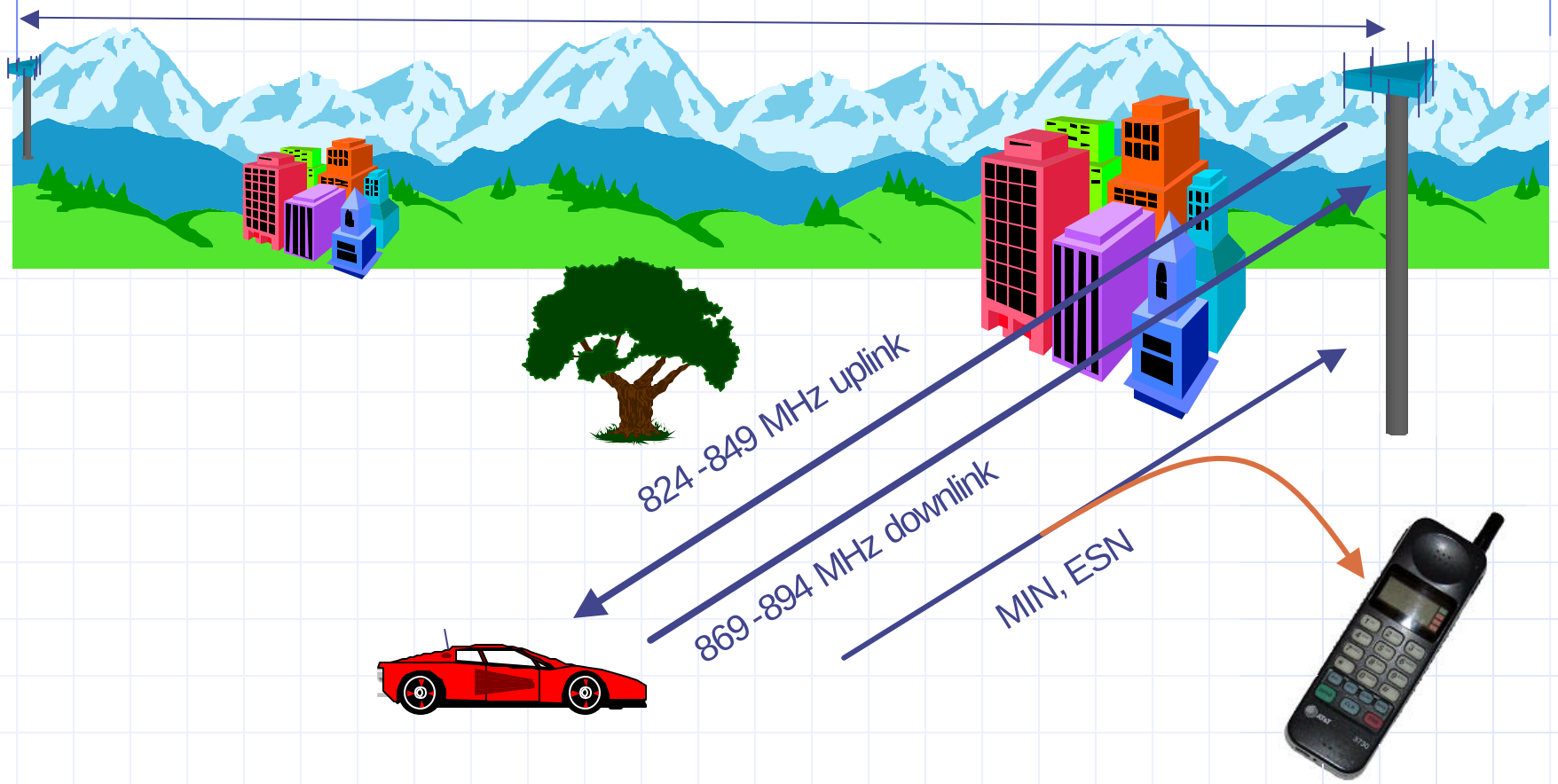
- Case 1:
  - Interception – compromise of confidentiality
- Case 2:
  - Interception – compromise of authentication methods, theft of service
- Case 3:
  - Interception – theft of service
  - Jamming – compromise of availability
- Case 4:
  - Interoperability issues – availability of servide,
  - interception – compromise of confidentiality
- Case 5:
  - Interception – compromise of confidentiality, compromise of authentication, theft of service,

Wireless System Compromise – Case 1: Terrestrial Microwave

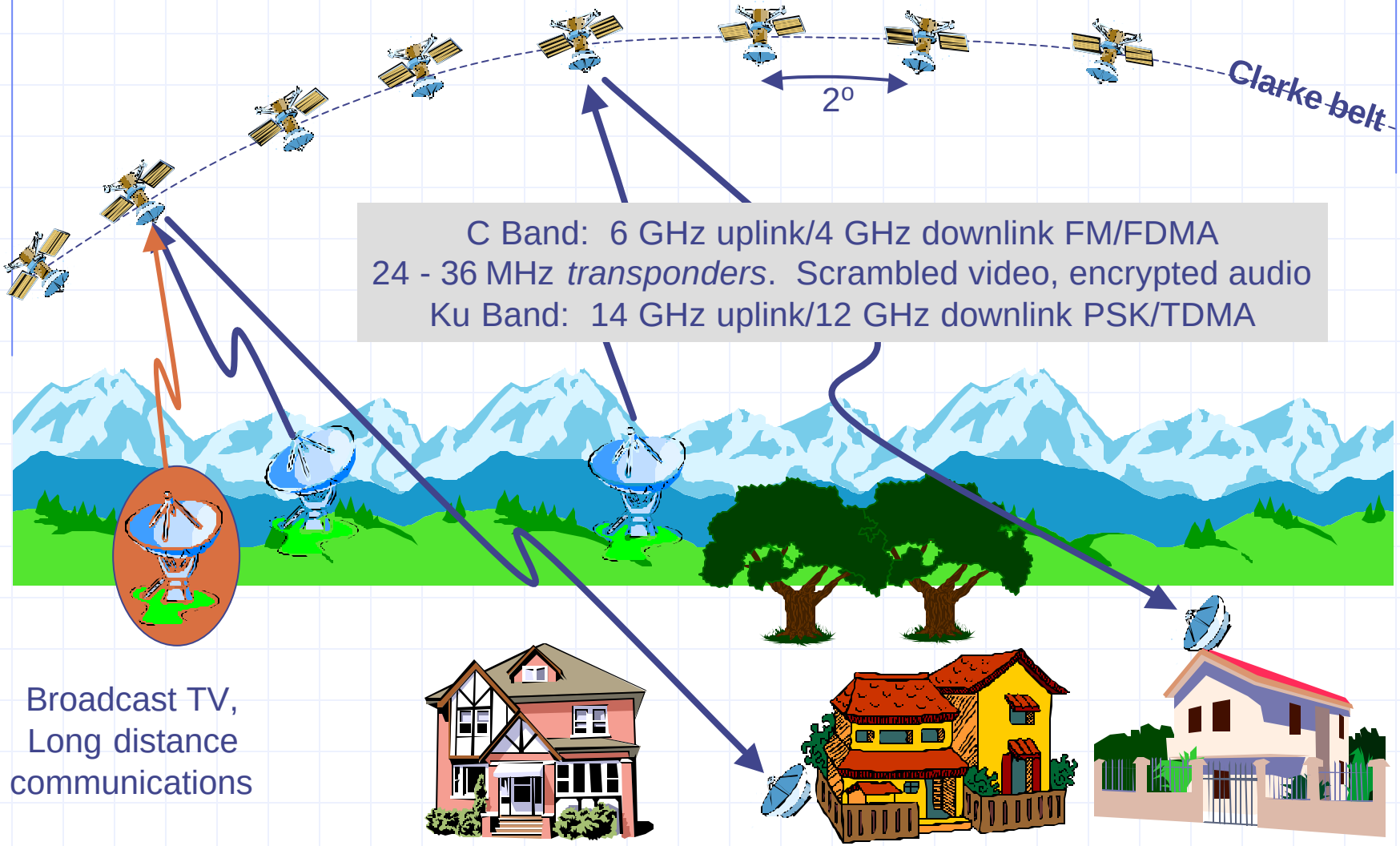


4 GHz
Analog SSB FDMA
Multichannel Voice traffic
CCS signaling
Washington, DC area

Wireless System Compromise – Case 2: Cellular Cloning



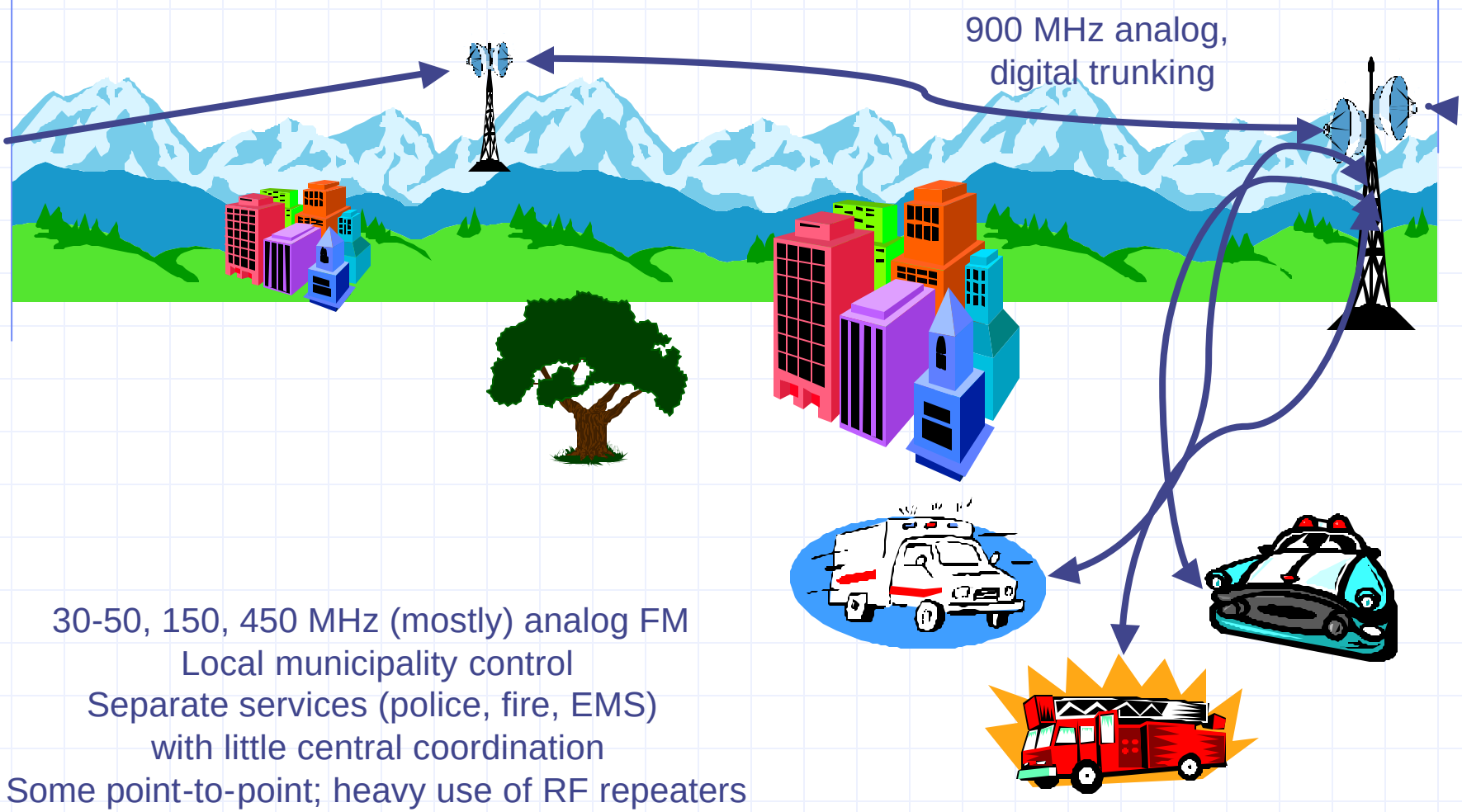
Wireless System Compromise – Case 3: Satellite Communications



C Band: 6 GHz uplink/4 GHz downlink FM/FDMA
24 - 36 MHz *transponders*. Scrambled video, encrypted audio
Ku Band: 14 GHz uplink/12 GHz downlink PSK/TDMA

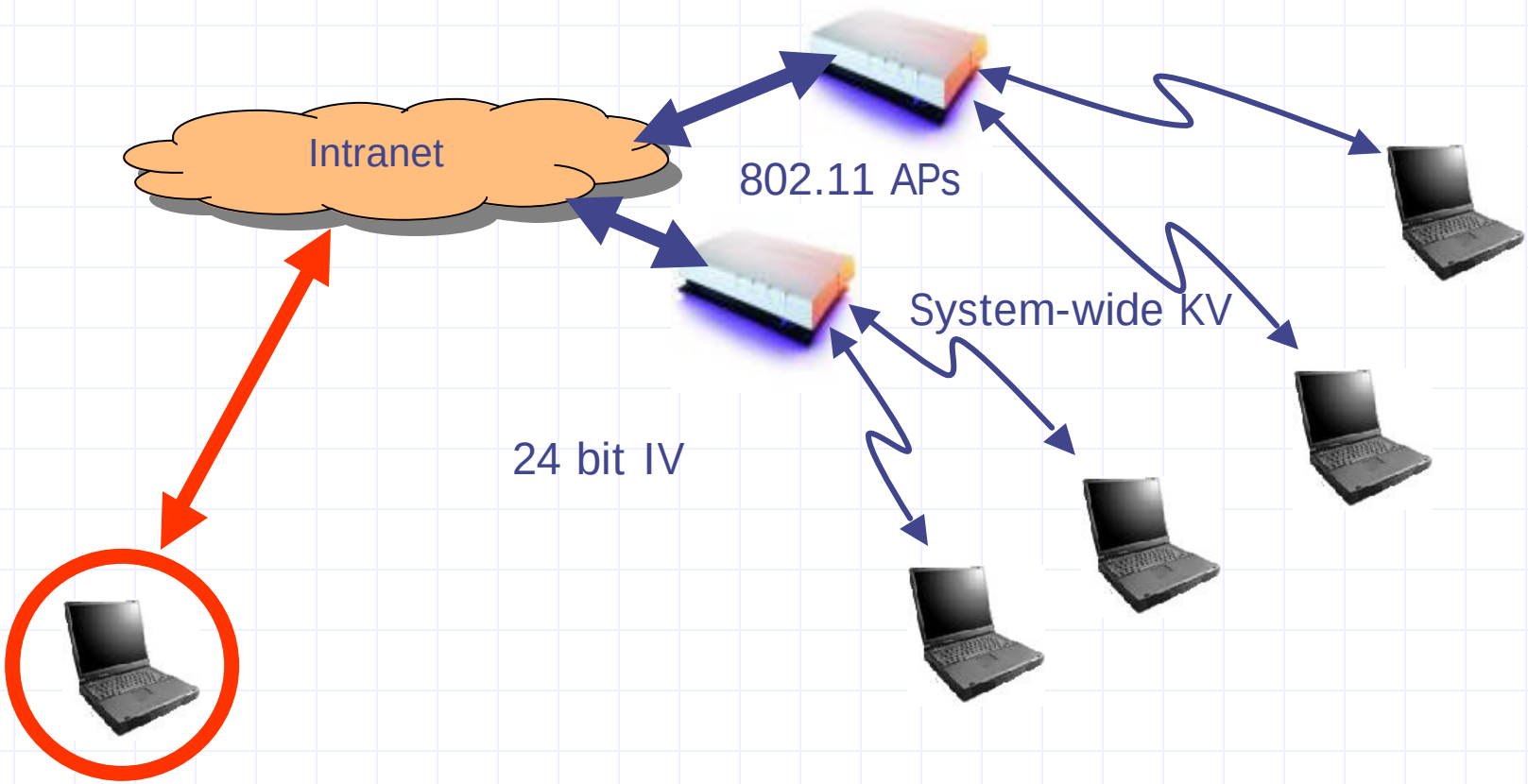
Broadcast TV, Long distance communications

Wireless System Compromise – Case 4: Public Safety Wireless



30-50, 150, 450 MHz (mostly) analog FM
Local municipality control
Separate services (police, fire, EMS)
with little central coordination
Some point-to-point; heavy use of RF repeaters

Wireless System Compromise – Case 5: Wireless LANs



A Short Primer on Cryptography

- Monoalphabetic cipher:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Permutation

BCDEFGHIJKLMNOPQRSTUVWXYZA

THIS IS A SECRET MESSAGE

UIJT JT B TFDSFU NFTTBHF

A Short Primer on Cryptography

- Monoalphabetic cipher:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Permutation

BCDEFGHIJKLMNOPQRSTUVWXYZA

THIS IS A SECRET MESSAGE

UIJT JT B TFDSFU NFTTBHF

A Short Primer on Cryptography

- Monoalphabetic cipher:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Permutation

BCDEFGHIJKLMNOPQRSTUVWXYZA

THIS IS A SECRET MESSAGE

UIJT JT B TFDSFU NFTTBHF

- Polyalphabetic cipher

THISSECRETMESSAGEWILLBEMUCHHARDERTOBREAK

+

HAHAHAHAHAHAHAHAHAHAHAHAHAHAHAHAHAHAHA

BIQTAFKSMUUFATIHMXQMTCMNCDPIISLFZUWCZFIL

A Short Primer on Cryptography

- Monoalphabetic cipher:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Permutation ↓

BCDEFGHIJKLMNOPQRSTUVWXYZA

THIS IS A SECRET MESSAGE ↓

UIJT JT B TFDSFU NFTTBHF

- Polyalphabetic cipher

THISSECRETMESSAGEWILLBEMUCHHARDERTOBREAK

\+

HAHAHAHAHAHAHAHAHAHAHAHAHAHAHAHAHAHAHA

↓

BIQTAFKSMUUFATIHMXQMTCMNCDPIISLFZUWCZFIL

=

B_Q_A_K_M_U_A_I_M_Q_T_M_C_P_I_L_Z_W_Z_I_

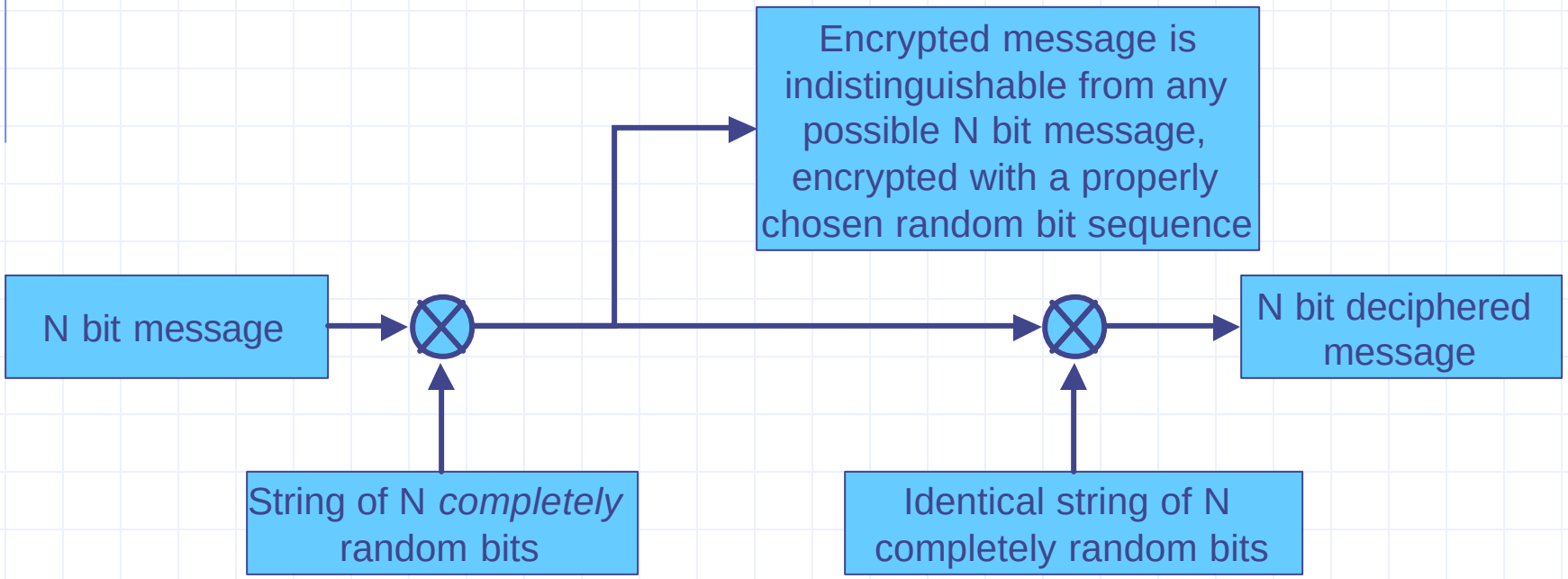
\+

_I_T_F_S_U_F_T_H_X_M_C_N_D_I_S_F_U_C_F_L

- Find periodicity
- Exploit redundancy

A Short Primer on Cryptography

- Key stream repetition is the weakness of a polyalphabetic cipher
  - What if the key stream never repeated?



- "One-time pad" is only provably secure cipher

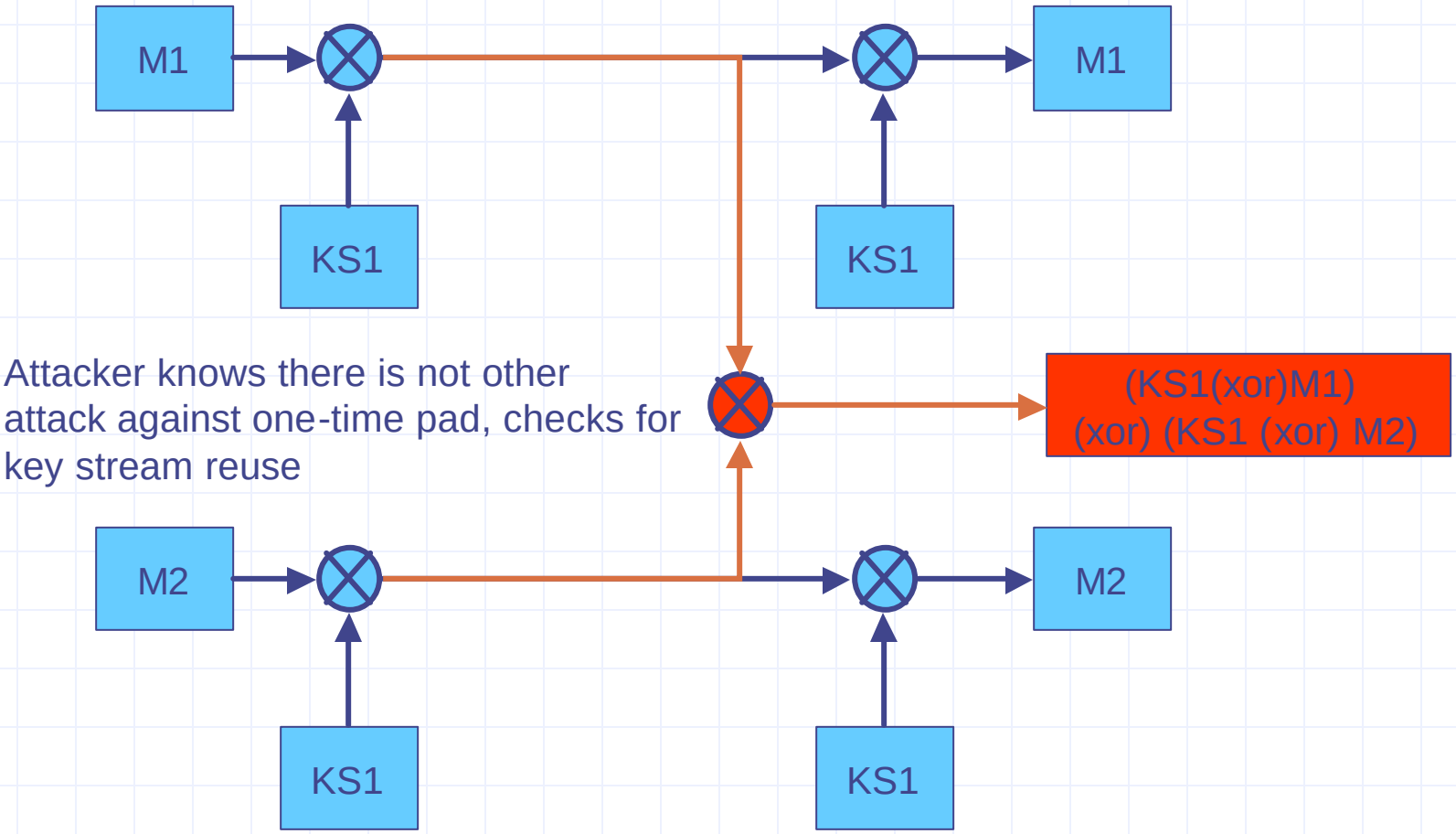
A Short Primer on Cryptography

- Compromise of the one-time pad

Sender accidentally sent M2,
reusing KS1, previously used for M1

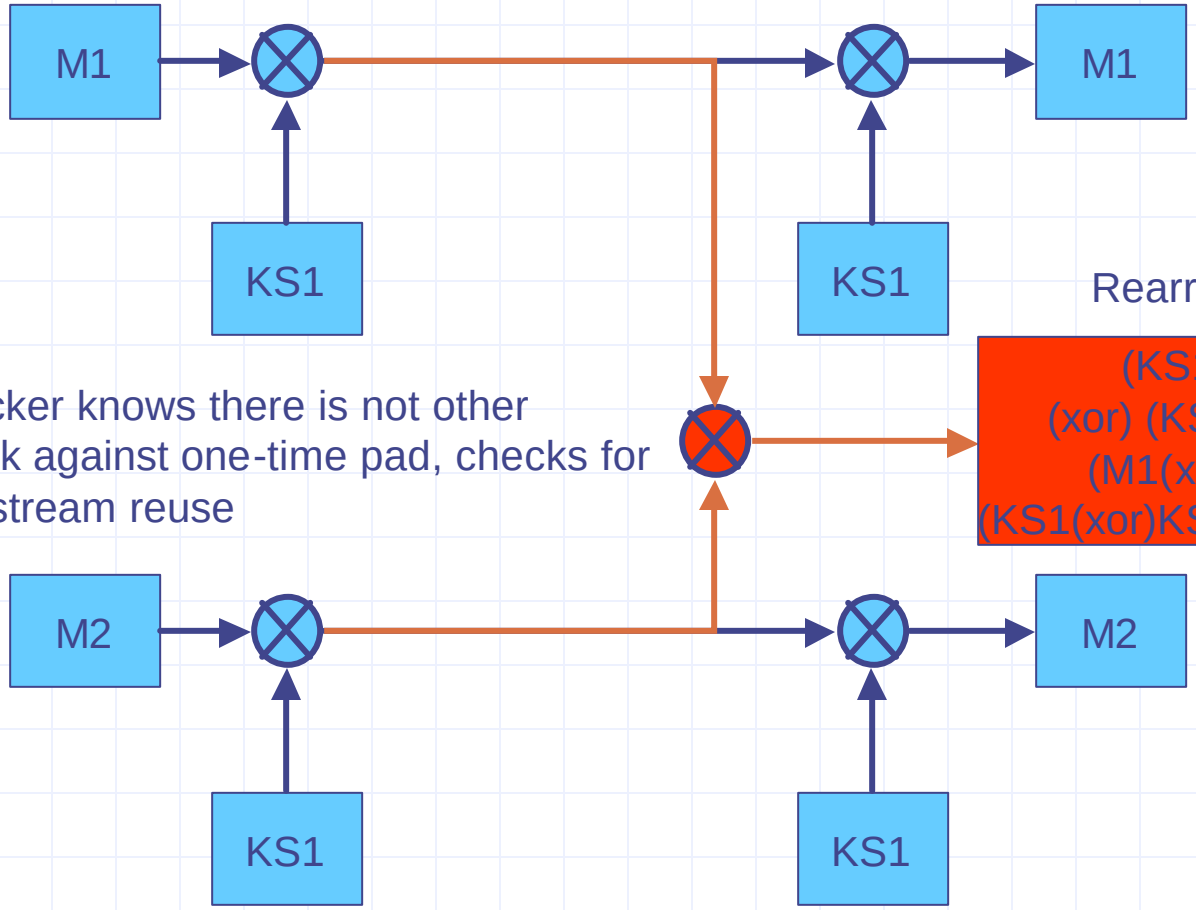
A Short Primer on Cryptography

- Compromise of the one-time pad



A Short Primer on Cryptography

- Compromise of the one-time pad

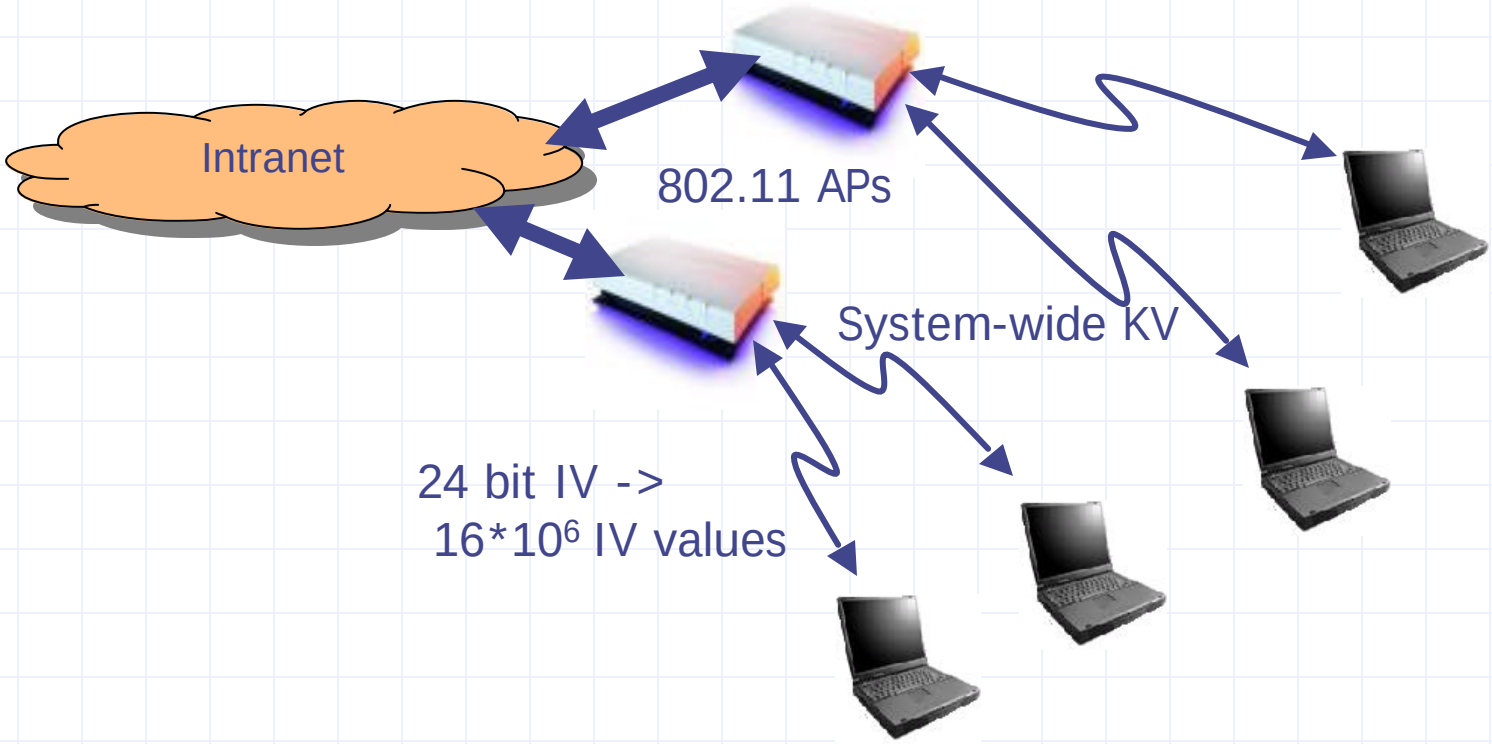


Rearranging terms:

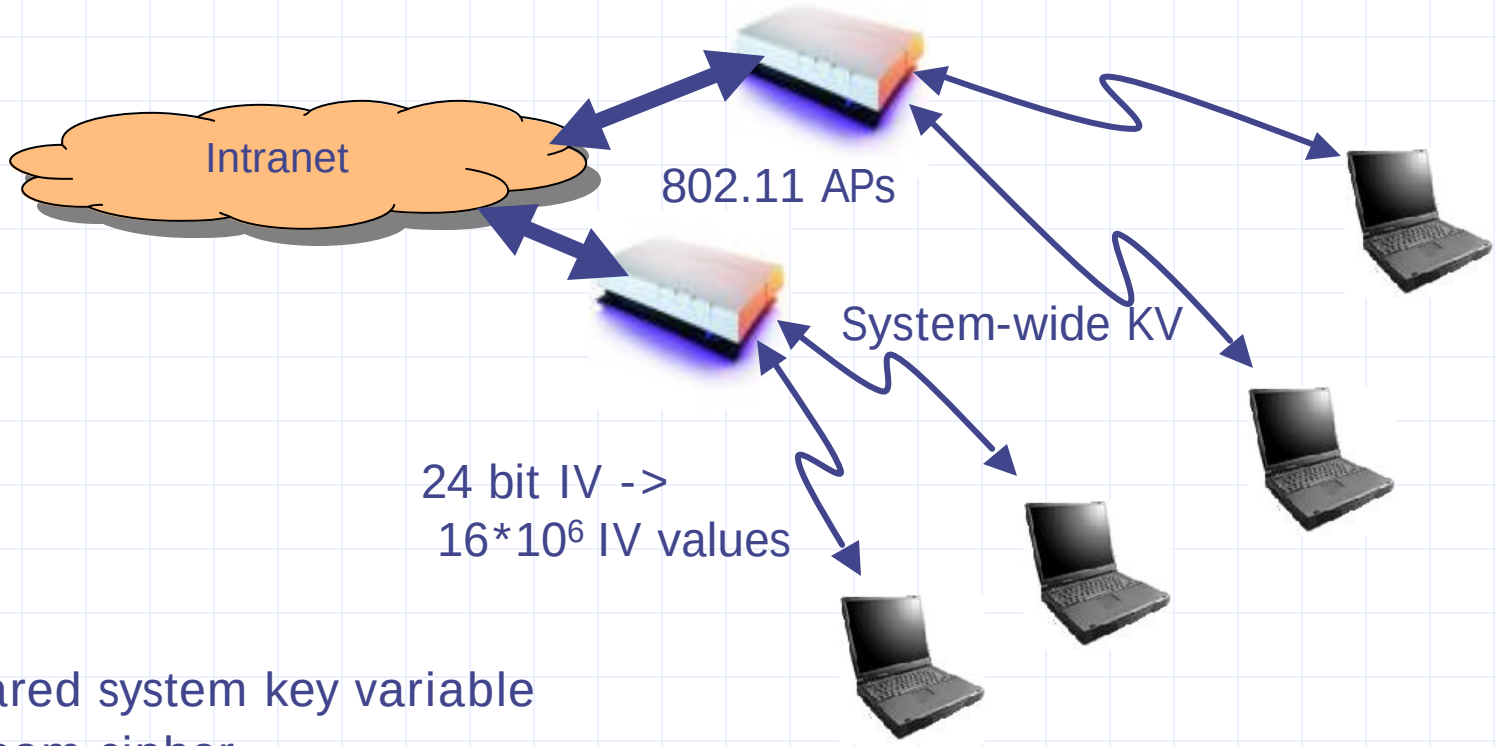
(KS1(xor)M1) (xor) (KS1 (xor) M2) = (M1(xor)M2) (xor) (KS1(xor)KS1) = M1 (xor) M2

This is a polyalphabetic cipher with M1 as key stream

What does this have to do with Wireless Security?



What does this have to do with Wireless Security?



- Shared system key variable
- Stream cipher
- Small IV space -> guaranteed IV collision
  - (16 million IV values, 10% utilization, 5Mb/s throughput, 500 byte packets) = ~36 hours)
- Fixed key + IV collision -> key stream reuse -> polyalphabetic attack
- Redundancy in plaintext doesn't help (e.g., plaintext checksum)

What went wrong?

- Either:
  - System design did not address security issues
  - System design did not anticipate threat environment
  - System design did not anticipate evolution of threat environment
  - System was stressed beyond its design limits

Göedel's Theorem:

- A self-consistent formal system must have theorems for which correctness cannot be proven
- Or, a consistent system cannot be complete

Security Implications of Gödel's Theorem:

- A self-consistent formal system must have theorems for which correctness cannot be proven
- Or, a consistent system cannot be complete

- A system security specification should be self-consistent – therefore it can't also be complete!
- My conjecture: For a sufficiently complex system, there is no *last* security hole (or software bug, or design flaw, …)

Security Implications of Gödel's Theorem:

- A self-consistent formal system must have theorems for which correctness cannot be proven
- Or, a consistent system cannot be complete

- A system security specification should be self-consistent – therefore it can't also be complete!
- My conjecture: For a sufficiently complex system, there is no *last* security hole (or software bug, or design flaw, …)

- Does Gödel suggest that these compromises are inevitable?

80/20 Rule – The Pareto Principle

- “80% of the resources of a country (or system, organization, …) are controlled by 20% of the users”

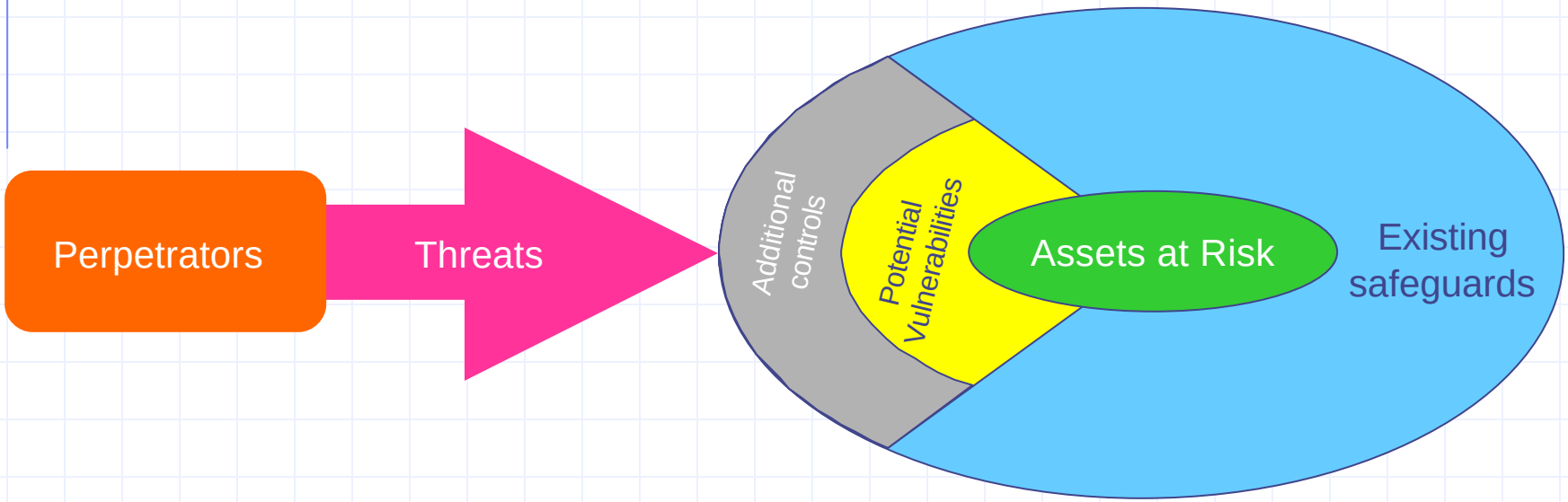
Quality Implications of The Pareto Principle

- "80% of the resources of a country (or system, organization, …) are controlled by 20% of the users"
- Quality: The majority of system faults are created by a small minority of the root causes

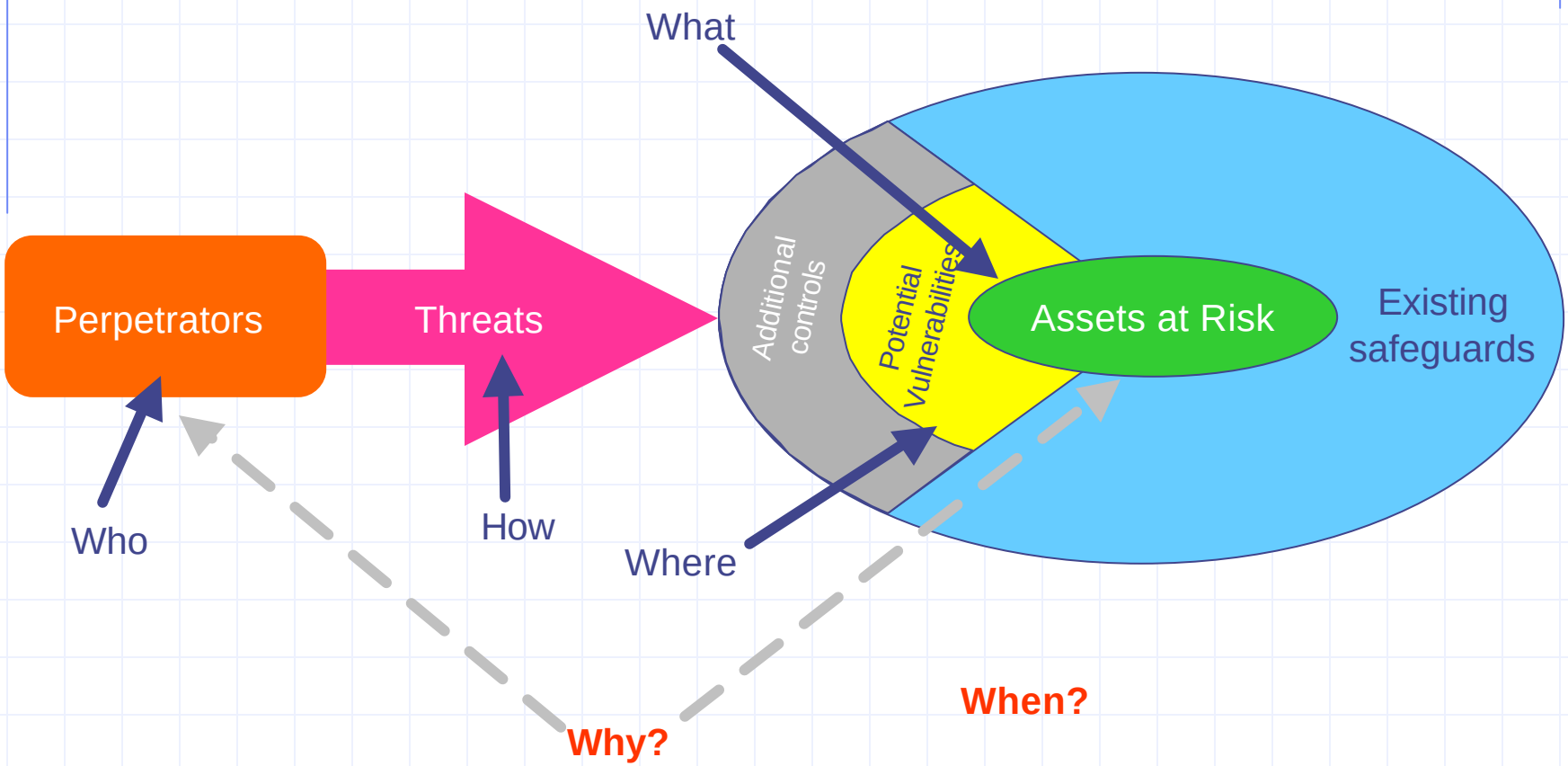
Quality and Security Implications of The Pareto Principle

- "80% of the resources of a country (or system, organization, …) are controlled by 20% of the users"
- Quality: The majority of system faults are created by a small minority of the root causes
- Security: The majority of system security attacks are created by a small minority of security design flaws
  - We don't have to find all the security flaws, just the most damaging ones
    - Cost-benefit analysis + threat analysis

Security Assessment



Security Assessment



More Lessons from Quality: Continuous Process Improvement

- Identify defects
- Find “low-hanging fruit”
- Identify root cause
- Search for commonality of systemic issues
- Correct problem(s)
- Add lesson to design process
- Repeat

Conclusion

- Wireless Security is not an oxymoron
- Wireless access creates different, but not new, issues in system design
- Potential for jamming or undetected interception are greater for wireless systems
- Thorough examination of security considerations in design of complex ~~wireless communications~~ systems is needed, early in the design cycle

Future Research Directions

- **Identification** and **Authentication** techniques that do not compromise user.
- MIMO, Smart Antenna techniques for improved system **Availability**
- Location-based and RF signature techniques for terminal **Identification**
- Applicability of wideband modulation techniques to mitigate (intentional) interference to improve **Availability**
- Key management infrastucture for mobile data networking