FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

Stochastic Message Authentication

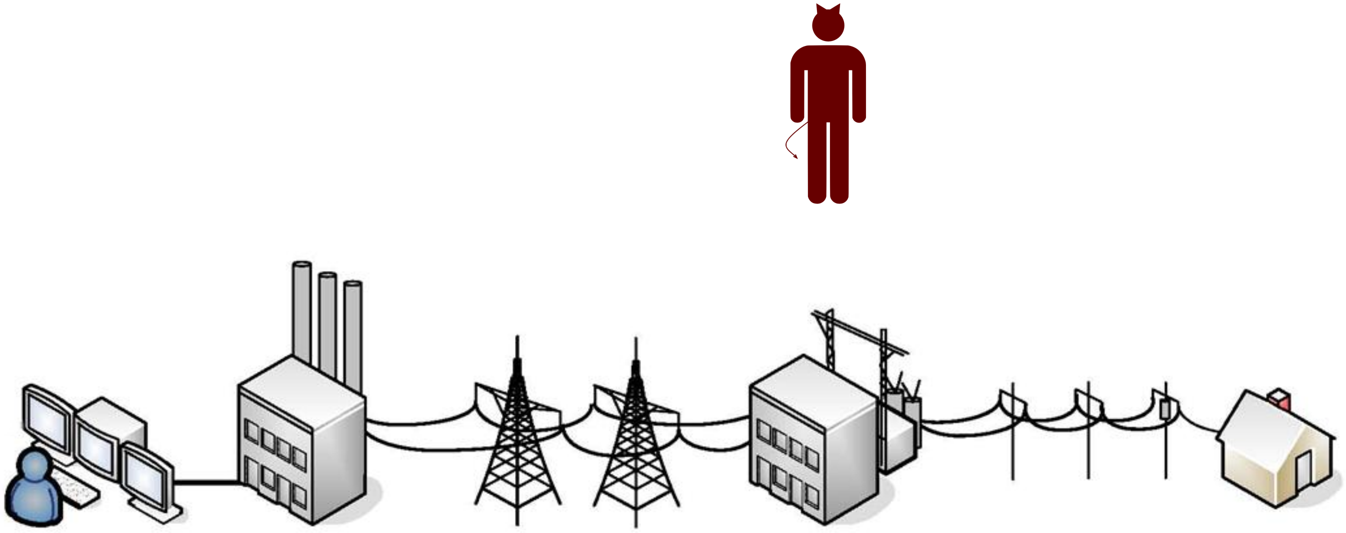
Aron Laszka, Yevgeniy Vorobeychik, Xenofon Koutsoukos

Vanderbilt University

Berkeley UNIVERSITY OF CALIFORNIA
Massachusetts Institute of Technology
NSF
MICHIGAN
VANDERBILT UNIVERSITY

Motivation

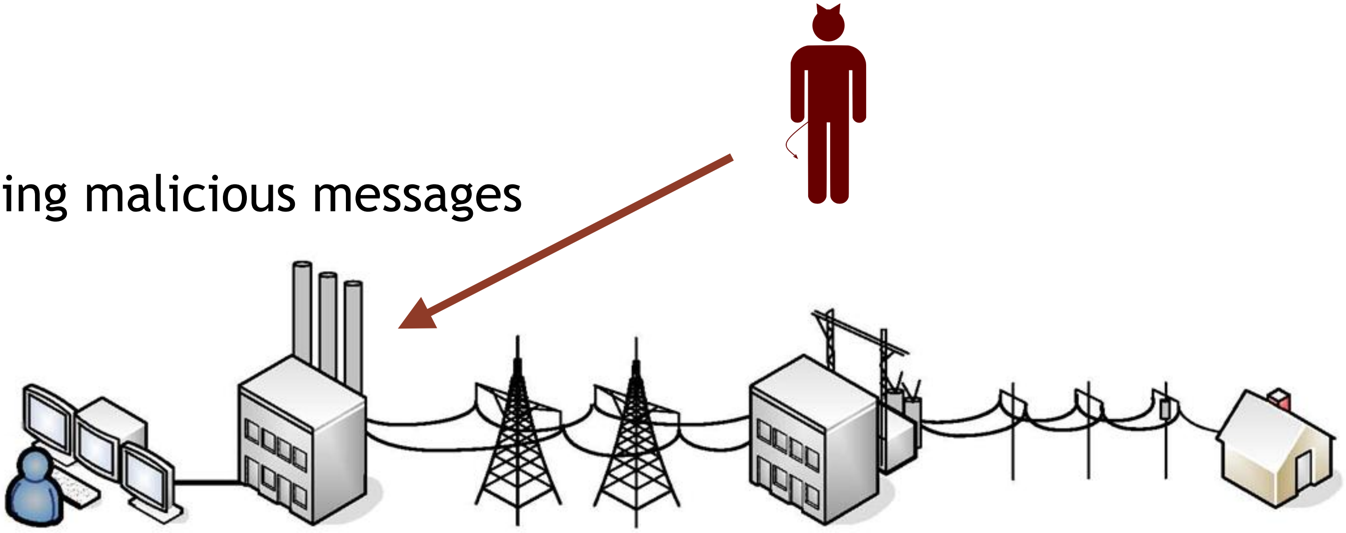
- Attacks against networked cyber-physical systems
  - e.g. smart grid



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

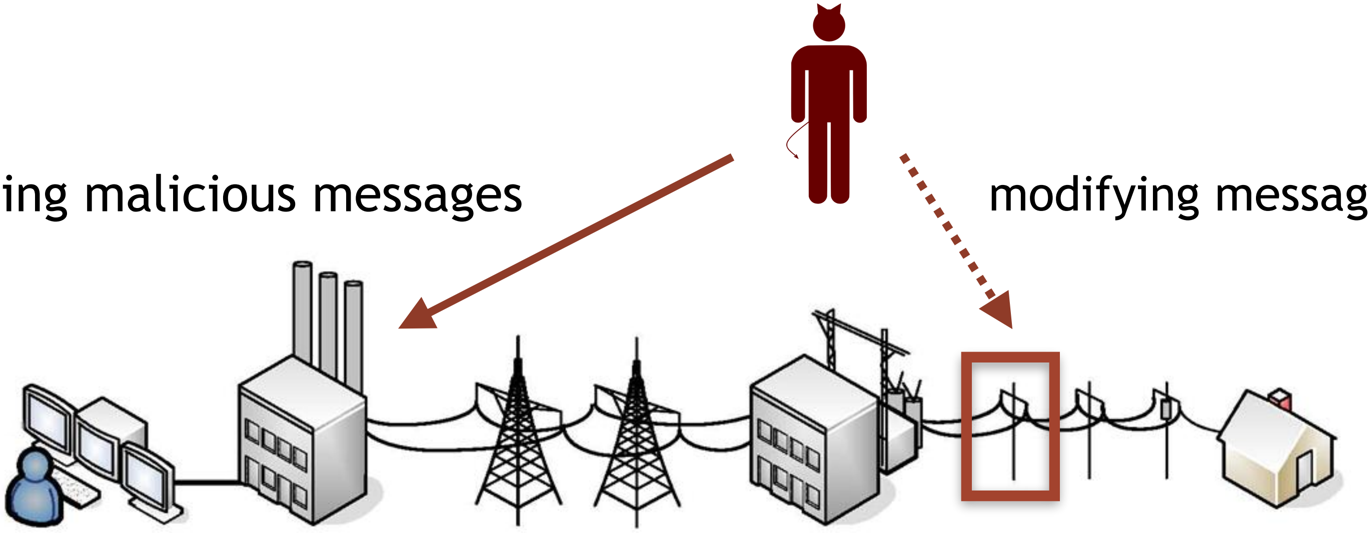
Motivation

- Attacks against networked cyber-physical systems
  - e.g. smart grid



Motivation

- Attacks against networked cyber-physical systems
  - e.g. smart grid

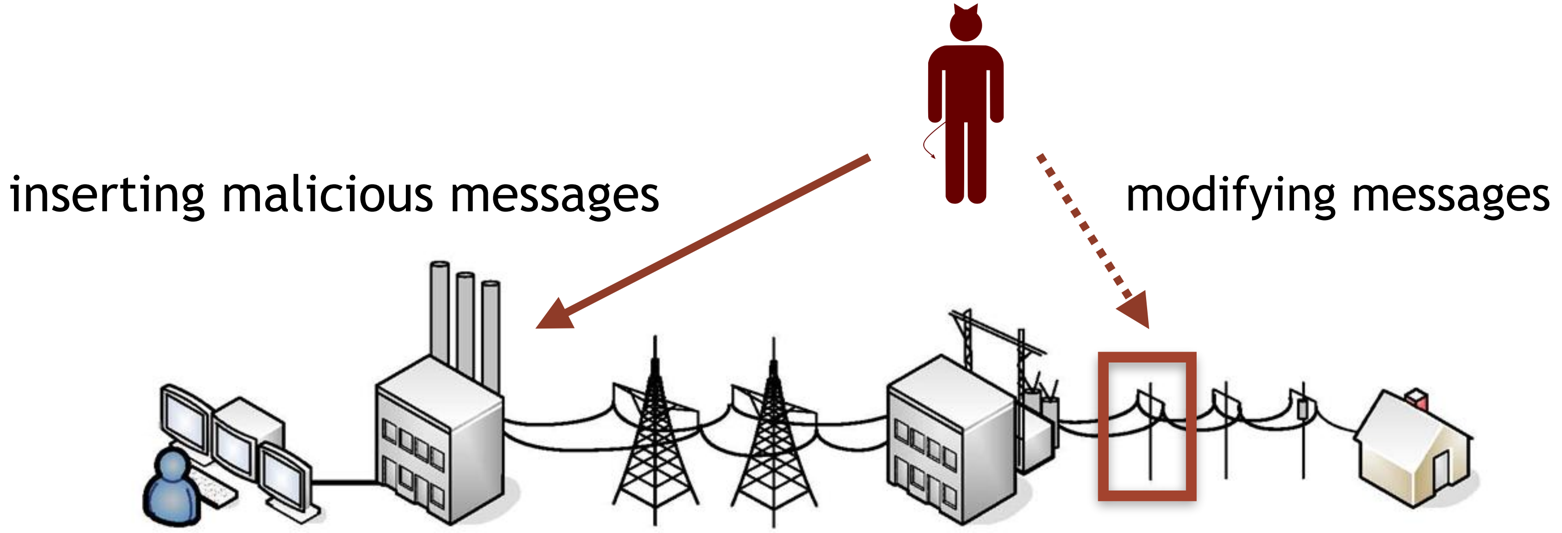


inserting malicious messages

modifying messages

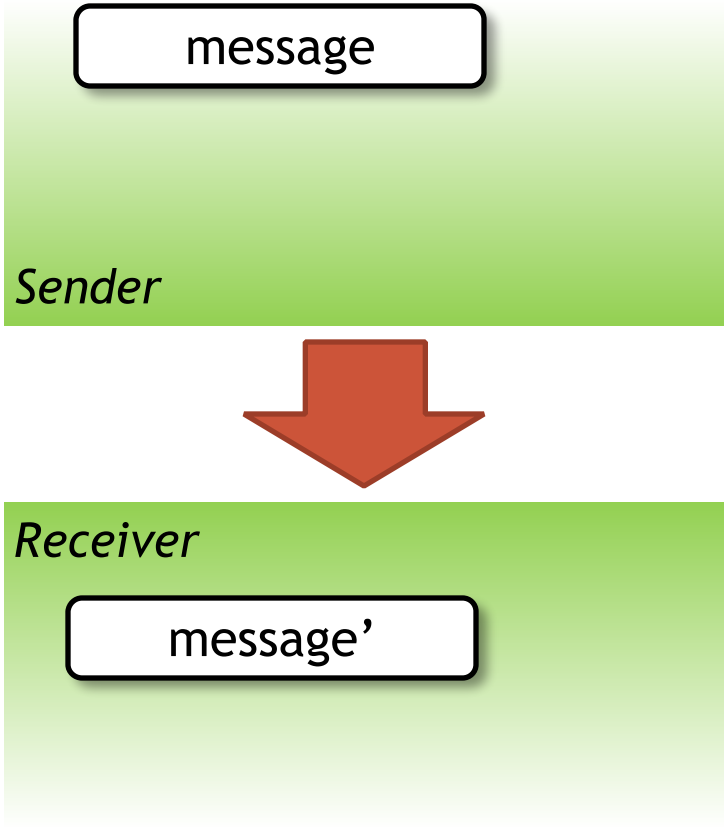
Motivation

- Attacks against networked cyber-physical systems
  - e.g. smart grid



We need to be able to **verify** the **integrity** and **authenticity** of messages!

Message Authentication



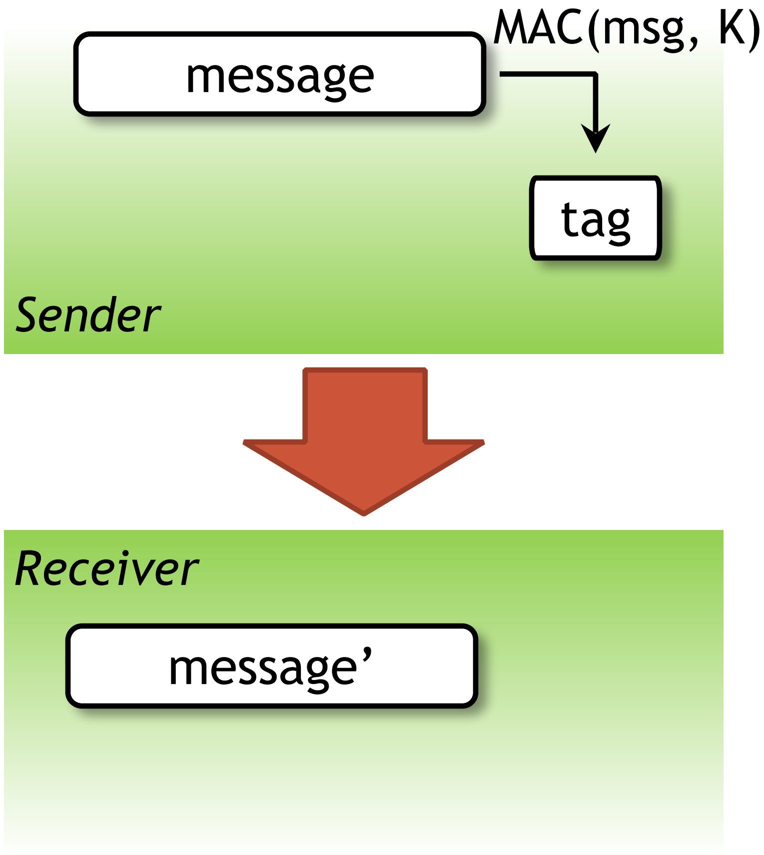
message

Sender

Receiver

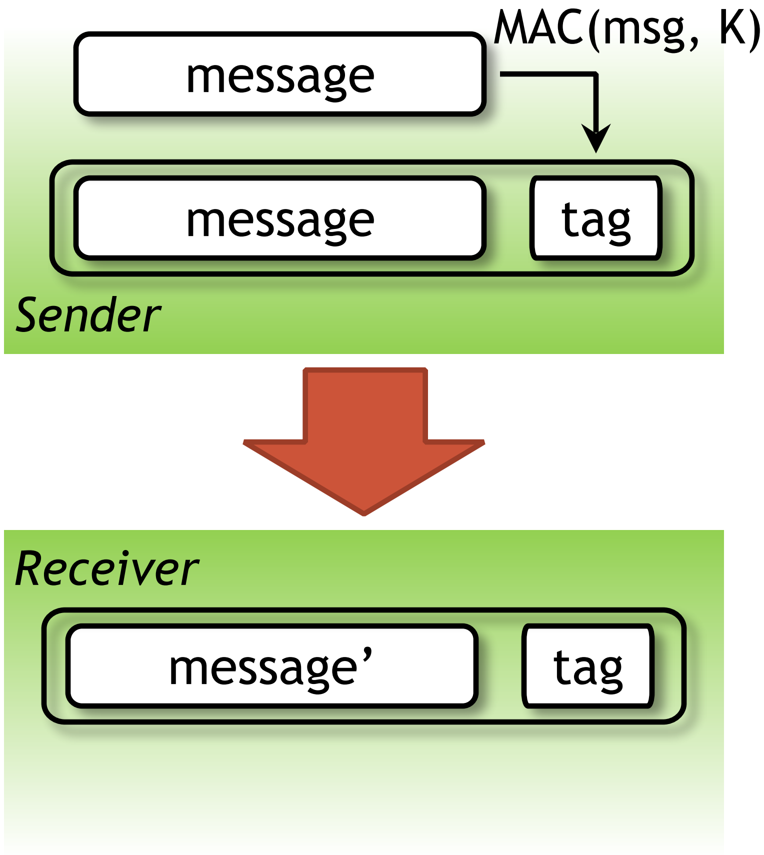
message’

Message Authentication



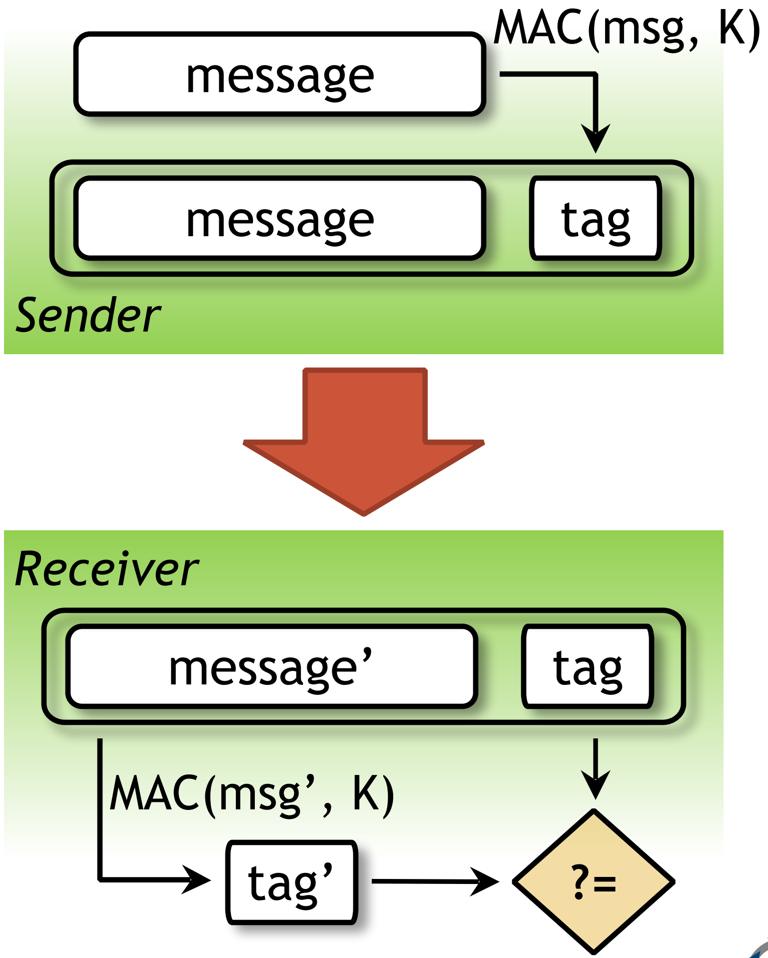
- For each message, sender computes an “authentication tag” using a secret key

Message Authentication



- For each message, sender computes an “authentication tag” using a secret key
- Adversary cannot forge a correct tag without knowing the key

Message Authentication



- For each message, sender computes an “authentication tag” using a secret key
- Adversary cannot forge a correct tag without knowing the key
- Receiver can verify the integrity and authenticity of the messages using the same key → detect any attack

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Challenges and Our Approach

- Computational demand of cryptographic primitives can be too high for **resource-bounded** devices
  - legacy devices in supervisory control systems
  - embedded or battery-powered devices (RFID tags, sensors)

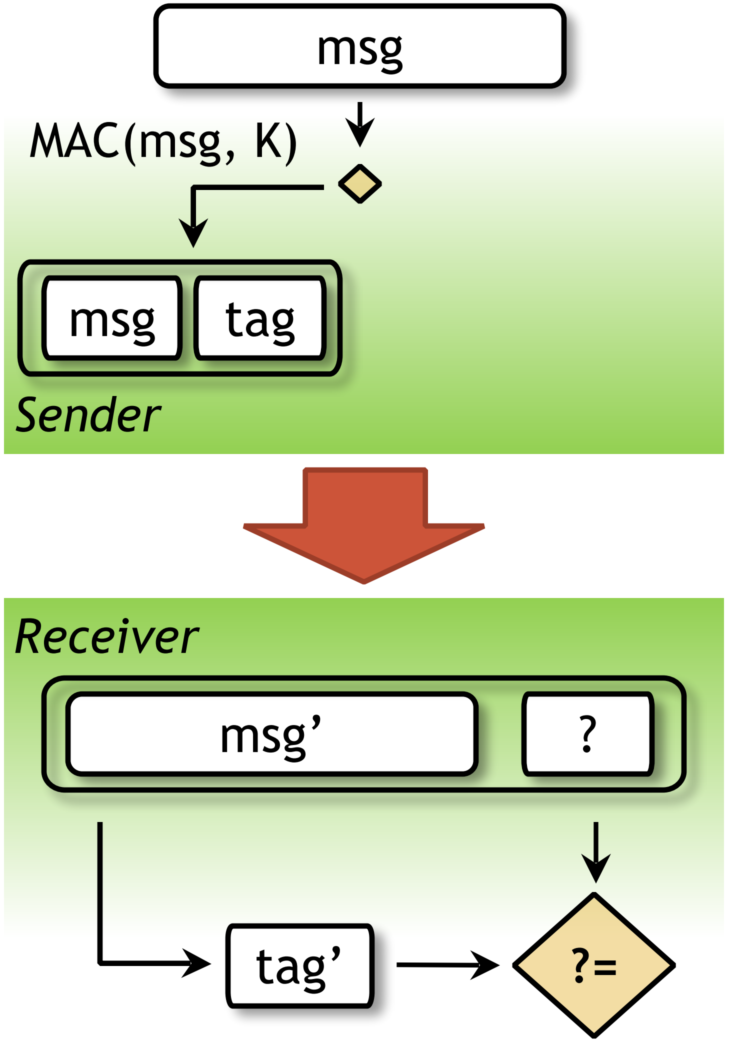
Challenges and Our Approach

- Computational demand of cryptographic primitives can be too high for **resource-bounded** devices
  - legacy devices in supervisory control systems
  - embedded or battery-powered devices (RFID tags, sensors)
- "Lightweight" cryptographic primitives
  - Decision to secure a system is still **binary**: either security is employed, incurring some fixed overhead, or it is not

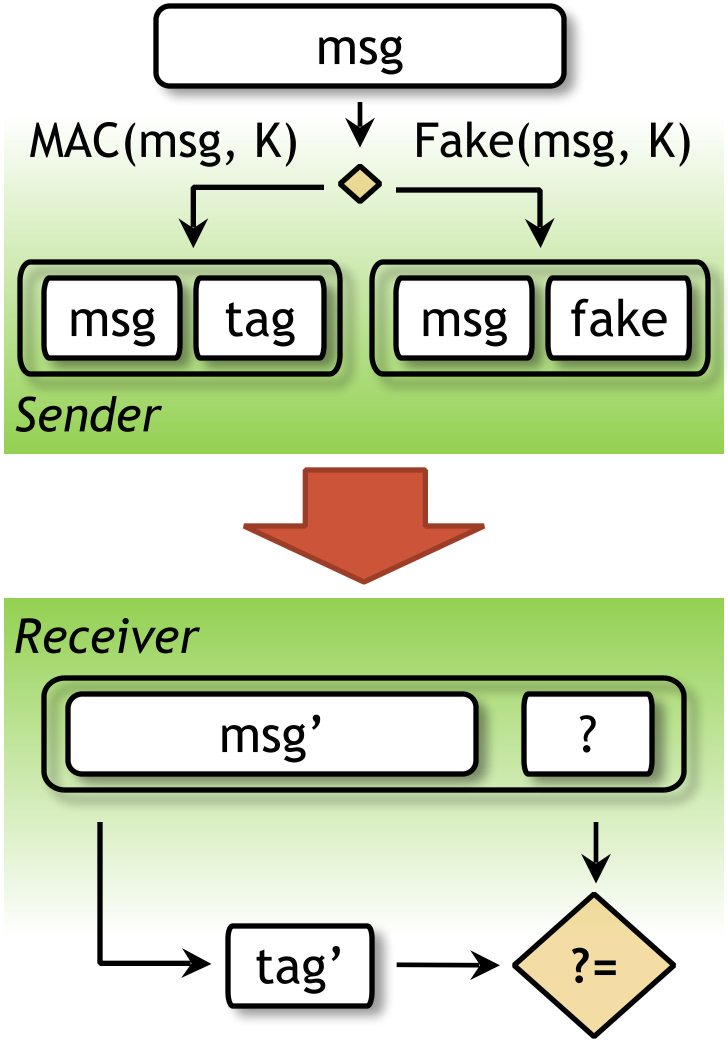
Challenges and Our Approach

- Computational demand of cryptographic primitives can be too high for **resource-bounded** devices
  - legacy devices in supervisory control systems
  - embedded or battery-powered devices (RFID tags, sensors)
- “Lightweight” cryptographic primitives
  - Decision to secure a system is still **binary**: either security is employed, incurring some fixed overhead, or it is not
- Our approach:
  general-purpose framework for trading off security and computational demand using an existing MAC scheme
  → best-possible security for **arbitrary resource-bound**

Stochastic Message Authentication

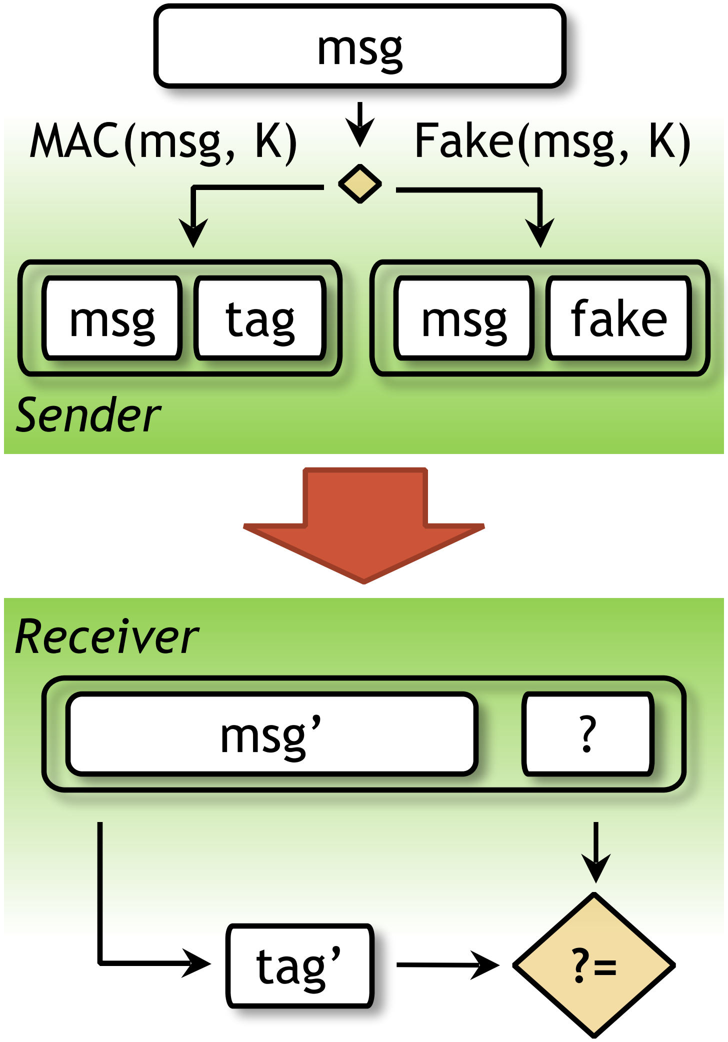


Stochastic Message Authentication



- For some messages, the sender computes a “fake tag”, which is computationally less demanding, but does not protect integrity

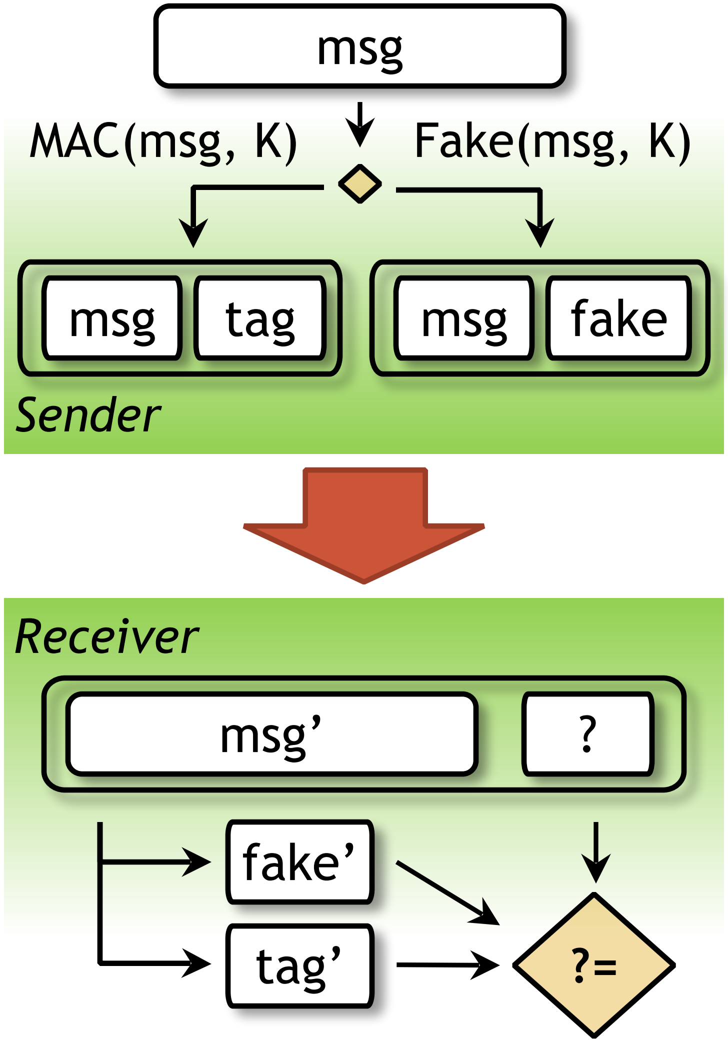
Stochastic Message Authentication



- For some messages, the sender computes a "fake tag", which is computationally less demanding, but does not protect integrity
- Adversary cannot distinguish fake tags from correct tags

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Stochastic Message Authentication



- For some messages, the sender computes a "fake tag", which is computationally less demanding, but does not protect integrity
- Adversary cannot distinguish fake tags from correct tags
- Receiver can verify if a message has a fake or a correct tag efficiently → detect attacks with high probability

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Game-Theoretic Model

- Stackelberg security game
  - we divide messages into C classes based on their potential to cause damage

	Defender	***Attacker***
Strategy choice	*for each class c, the probability of authentication p_c*	*for each class c, the number of modified / inserted messages a_c*

Game-Theoretic Model

- Stackelberg security game
  - we divide messages into C classes based on their potential to cause damage

	Defender	***Attacker***
Strategy choice	*for each class c, the probability of authentication p_c*	*for each class c, the number of modified / inserted messages a_c*
Detection probability	$1 - \prod_{c} (1 - p_c)^{a_c}$	

Game-Theoretic Model

- Stackelberg security game
  - we divide messages into C classes based on their potential to cause damage

		Defender	*Attacker*
Strategy choice		*for each class* c, *the probability of authentication* p_c	*for each class* c, *the number of modified / inserted messages* a_c
Detection probability		$1 - \prod_c (1 - p_c)^{a_c}$	
Payoff	*attack undetected*	*loses amount of damage, i.e.,* -$\sum a_c L_c$	*gains amount of damage, i.e.,* $\sum a_c L_c$

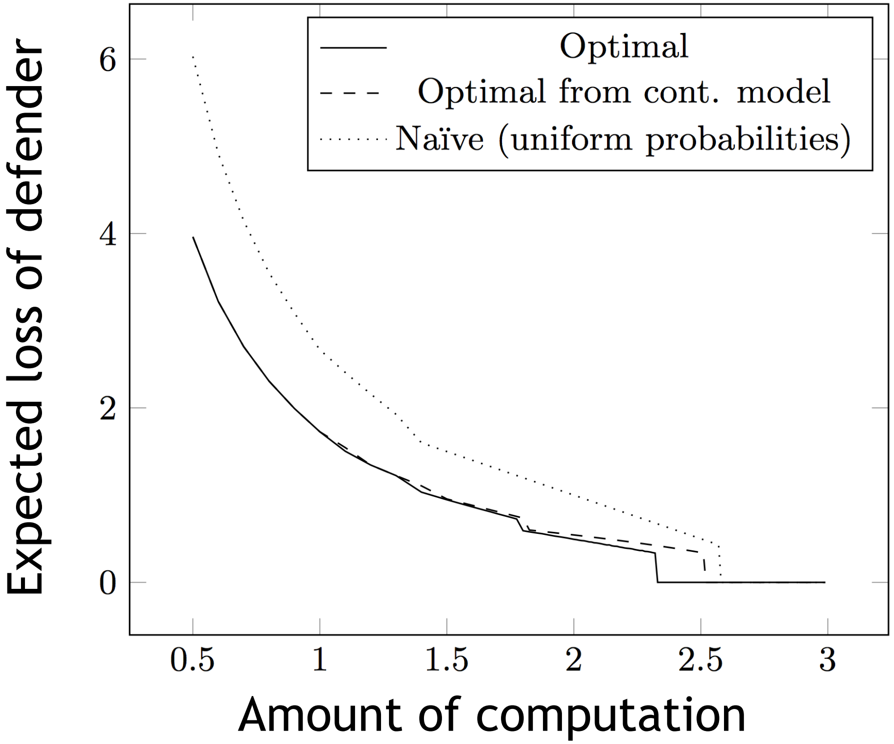
Game-Theoretic Model

- Stackelberg security game
  - we divide messages into C classes based on their potential to cause damage

		Defender	*Attacker*
Strategy choice		*for each class c, the probability of authentication p_c*	*for each class c, the number of modified / inserted messages a_c*
Detection probability		$1 - \prod_c (1 - p_c)^{a_c}$	
Payoff	*attack undetected*	*loses amount of damage, i.e., -$\sum a_c L_c$*	*gains amount of damage, i.e., $\sum a_c L_c$*
	attack detected	*zero*	*“punishment” -F*

Theoretical Results

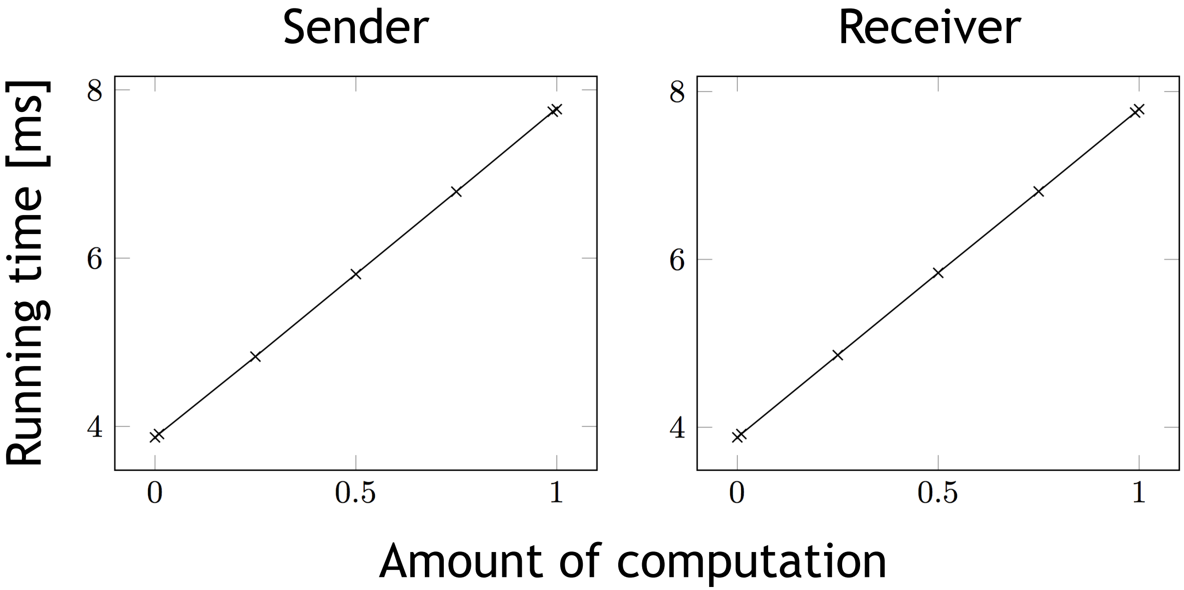
- Game-theoretic model of stochastic message authentication
  - Finding optimal authentication strategy

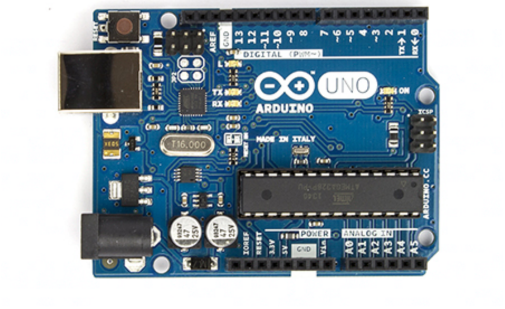


✓ trade-off between computation and security

Practical Results

- Proof-of-concept implementation using SHA-1 HMAC on an `ATmega328P` microcontroller





✓ for arbitrary resource bound

Thank you for your attention!

Questions?

Aron Laszka
aron.laszka@vanderbilt.edu
Yevgeniy Vorobeychik
yevgeniy.vorobeychik@vanderbilt.edu
Xenofon Koutsoukos
xenofon.koutsoukos@vanderbilt.edu