


Long-Lived Authentication Protocols for Critical Infrastructure Process Control Systems

Rasika Chakravarthy, Carl Hauser,
David E. Bakken

Washington State University
March 15, 2010

[Outline]

- Introduction
- Context
- Protocols
- Future Work and Conclusion



Introduction

Toward more flexible and secure PCS

- Today: retro-fitting existing SCADA systems for security
- Near future: creating new monitoring and control networks with
 - More bandwidth
 - Lower latency
 - More automated controls
- Want security built-in rather than bolted-on

[Cryptography ages]

- Algorithms and keys considered secure in one decade are not in the next
 - Increasing computational power for brute-force attacks
 - Research discovers new faster-than-brute-force attacks
- A problem for long-lived, widely distributed process control infrastructures

[Plan for the talk]

- Context: monitoring the electric power grid
- Long-term security: a modular, evolvable approach to authentication
- Related security challenges in this context



Context

[Electric Power Grids]

- Electric power grid
 - Continental scale
 - Thousands of independent companies, and agencies (utilities, generators, customers, ...)
 - A few coordinators (ISO, RTO)
- Monitoring and control
 - Today: utility-centric, human operators
 - Future: more automated, based on wide-area monitoring data

[Current practice]

- Low-speed links
 - Substation to control center
 - Challenge: low-latency security
- Inter-control center links
 - Point-to-point Internet-based VPNs
 - Case-by-case establishment

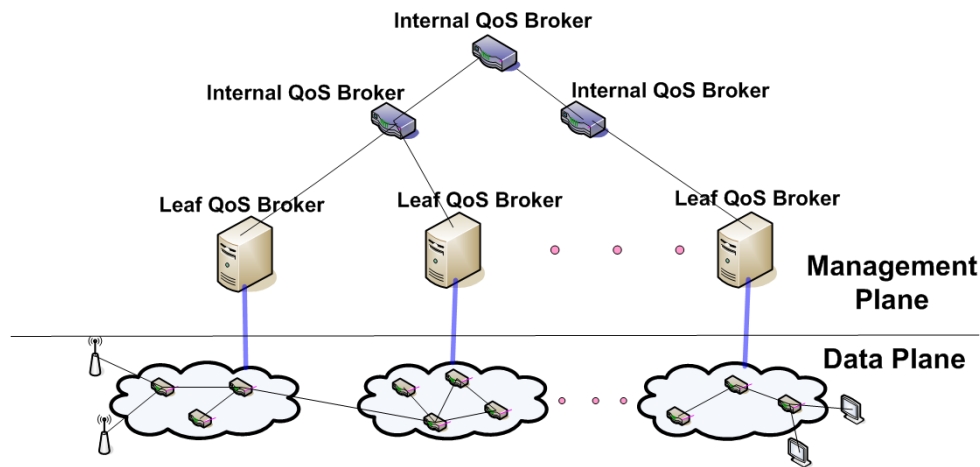
[Future needs]

- Much greater data exchange
 - Anywhere-to-anywhere
 - High bandwidth
- Authenticated, timely data for automated control

GridStat

- Flat, publish-subscribe, multi-cast data plane with QoS
- Hierarchical management plane

GridStat Architecture



[Some Security Challenges]

- Remote, inaccessible components
- Longevity of the system
 - 20-40 years
 - Certainly outlive keys
 - May outlive algorithms
- How, then, to replace algorithms (modules) securely and remotely

[Observations]

- Hierarchical management: authenticate adjacent nodes (parent-child)
- Parents manage their children
- Authentication is *the* essential service for which module change is needed
 - Flexible confidentiality and integrity services can be built if authentication is achieved
- What if a key is compromised?
 - Pre-loaded key material, consumed over time

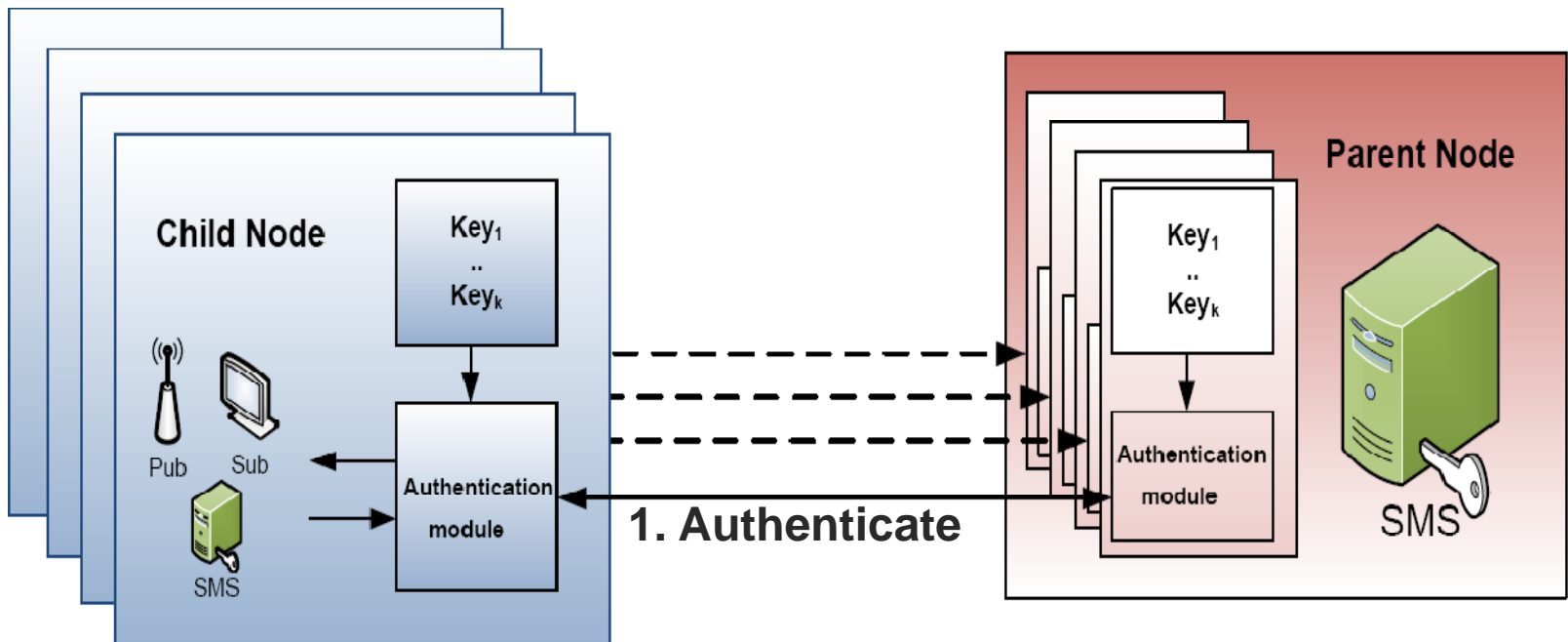
[Pre-loaded Key Material]

- Not Public Key Cryptography
 - Structure of keys depends on algorithm
 - Need to be flexible about algorithm
 - Worry about compromise of an “important” private key
- Symmetric Key Cryptography
 - No particular format for keys
- Distinct keys for every parent-child node pair

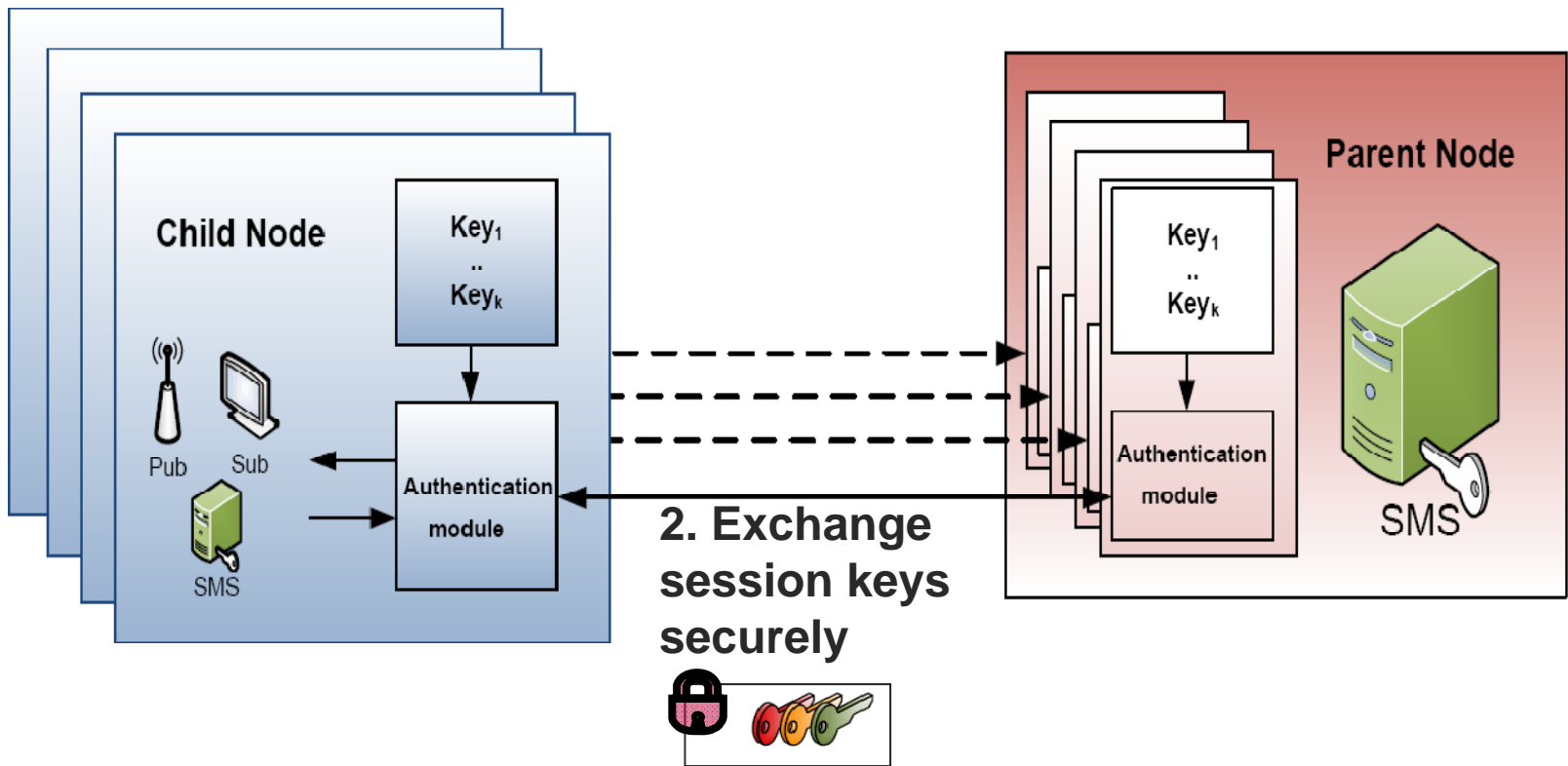


Protocols

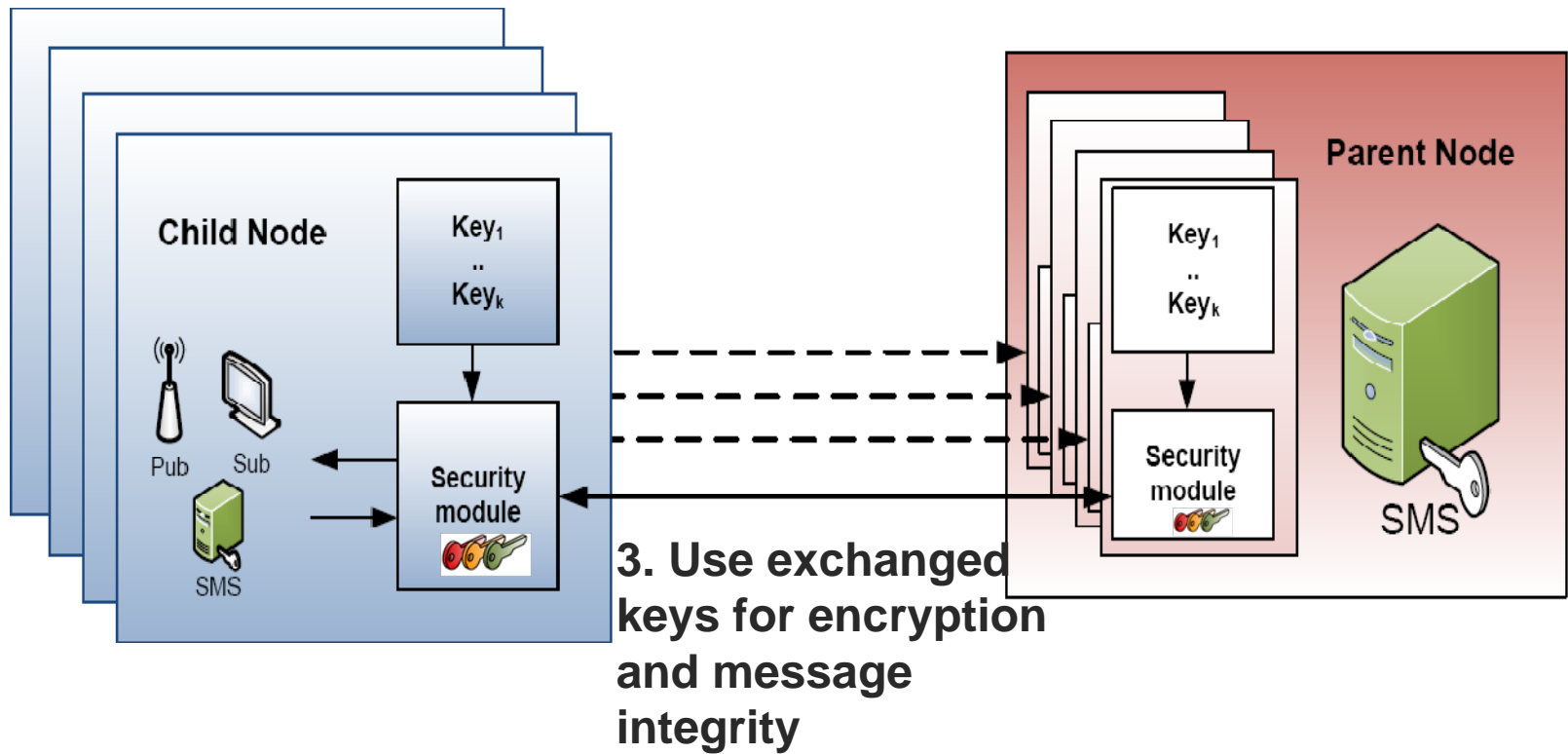
Authentication



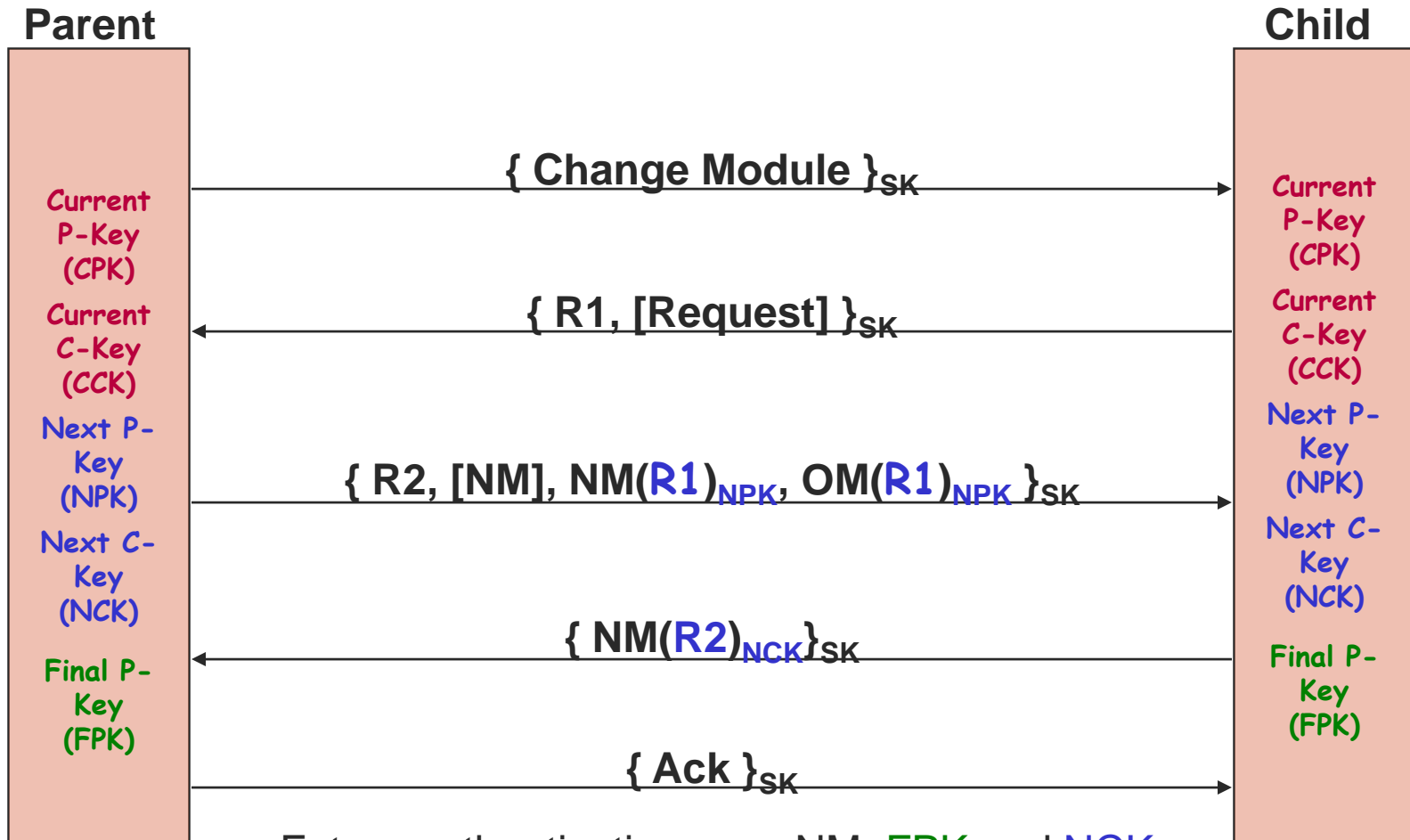
Key Exchange



Communicate



Module Change Protocol



Future authentications use NM, FPK and NCK

[Module Change Protocol]

- Authenticate initiator first
 - Use both old module and new module to test authenticity of initiator
 - False initiator may try to inject null new module
- Limit time between steps 1 and 4: ensure that attacker does not have time to break NPK due to its use with OM
 - Denial of service/exhaustion of keys attacks
- Change parent key after protocol since NPK was used with old module

Module Change Protocol - Failures

Response with Old Module	Response with New Module	Implication
Pass	Pass	Initiator successfully authenticated. Switch module
Pass	Fail	Possible breach in old module and/or key
Fail	Pass	New module malicious. No evidence of compromise
Fail	Fail	No evidence of compromise
Timeout before step 3		False initiation or delayed messages (report to parent)
Timeout before step 4		Delayed messages (parent restart)



Future work and conclusion

[Future Work]

- Practical use requires also
 - Protection of key material held in nodes
 - Enlarging the authentication scope
 - Moving from pair-wise parent-child authentication (management plane) to
 - Authenticated publisher-subscriber relationships (data plane)
 - Authorization
 - Message integrity and authentication
 - Low-latency multi-cast message authentication
 - Trust management

[Conclusion]

- Mutual session authentication – basis of confidentiality, message integrity and authenticity
- Long-lived authentication for management hierarchy
 - Authentication module change protocol
 - Based on
 - symmetric key encryption
 - pre-shared key material



Thank you

Authentication Protocol

