Research Spotlight Forum

8.6.19 Cybersecurity

Cybersecurity at NMSU: Cryptography and Cryptographic Protocols

PRESENTED BY:

Roopa Vishwanathan, CS Dept. at NMSU, roopav@nmsu.edu

SAND2019-9382 PE

ABOUT YOURSELF

- Brief Bio: Assistant Professor, CS Dept. NMSU since Fall'17. Before that Postdoc at UNC Greensboro, before that, PhD at University of North Texas (UNT)

- Research Areas: Cryptography, Security, Privacy

- Research Group Interests:
  - CrySPR Lab@CS dept@NMSU
  - 2 graduate students (MS), working on theoretical and applied cryptography
  - Demographic: international, 1 female
  - Past: 2 undergrad, domestic students

Keywords:

Cryptographic protocols, attribute-based cryptosystems, automated theorem proving, public ledgers

CURRENT WORK IN CYBERSECURITY

- Applied
  - Applying cryptographic protocols in blockchain-enabled applications
  - E.g., payment-based networks, credit networks such as Ripple
  - Accountability for entities conducting government surveillance
- Theoretical
  - Automated theorem proving of attribute-based cryptosystems and related protocols
  - Extended existing tools (AutoGnP) to support proofs of ABE and ABS

CURRENT WORK IN CYBERSECURITY: APPLIED CRYPTO

- **SAMPL**: **S**calable **A**uditability of **M**onitoring **P**rocesses using Public **L**edgers (ACM CCS 2019)
- Focus on government surveillance programs
- From cloak-and-dagger to more accountability
- Situation: Law enforcement gets warrant to conduct surveillance on companies' customers
- Problem: How to prevent law enforcement overreach? Companies over-sharing data?
- Several instances of overreach, companies sharing data casually (see DoJ OIG reports)

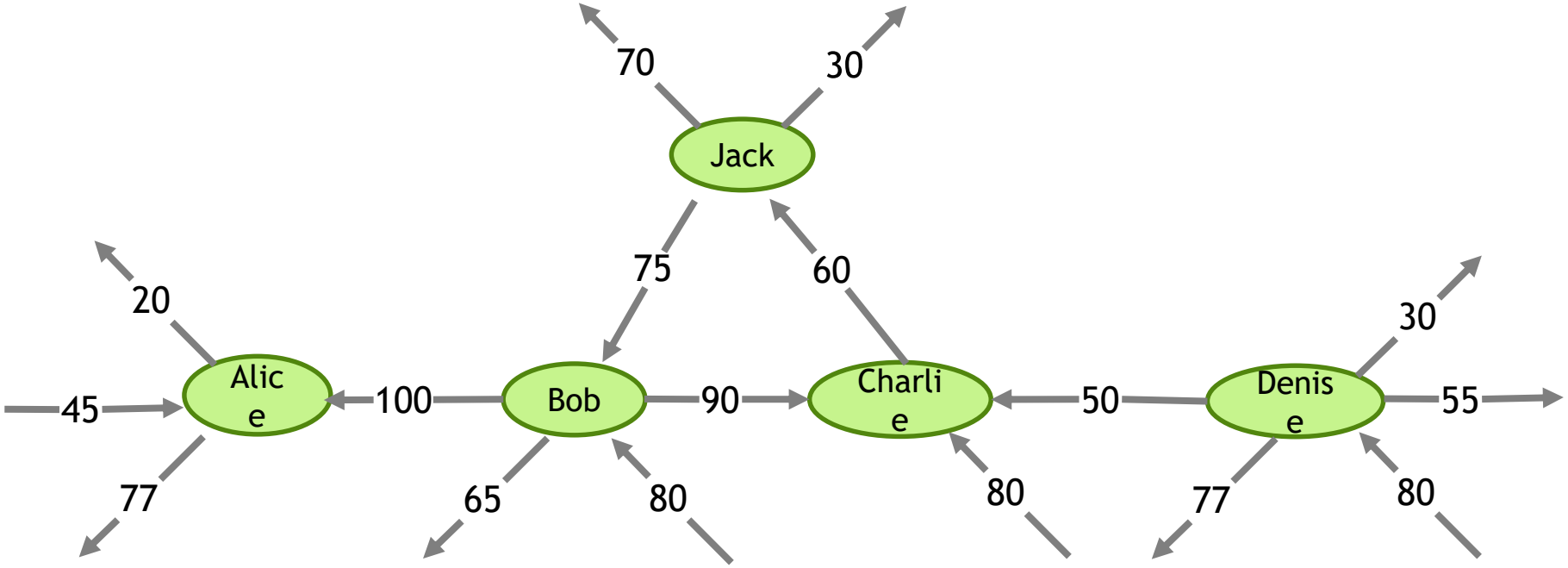
CURRENT WORK IN CYBERSECURITY: APPLIED CRYPTO

- ECPA, FISA, NSL: legal ways to conduct surveillance
- But who checks if legal guidelines followed?
- Our high-level solution: Introduce an *Enforcer*, who explicitly checks every surveillance request and response
- OIG can play role of *Enforcer*: be **proactive** rather than **reactive**
- Several cryptographic mechanisms employed: Pedersen commitments, zero-knowledge proofs, etc.

- Preliminary prototype. Several avenues for improvement...

CURRENT WORK IN CYBERSECURITY: APPLIED CRYPTO

BlAnC: **Bl**ockchain-based **An**onymous and Decentralized **C**redit Networks (ACM CODASPY 2019)



CURRENT WORK IN CYBERSECURITY: APPLIED CRYPTO

- Various Threats in Distributed Credit Networks
  - Misreport credit link weights
  - Relay fraudulent messages
  - Try to re-route payments
  - Choose not to respond to messages
  - Corrupt Intermediaries, a.k.a. "Landmarks"

- Our Contribution: **BlAnC**
  - User/transaction privacy, accountability, integrity
  - On-demand routing, concurrent transactions
  - Publicly identify malicious actors using blockchain
  - Use simple crypto primitives

CURRENT WORK IN CYBERSECURITY: Theory

- Cryptographic proofs increasingly complex, tedious to write/analyze, error-prone
  - Solution: Develop automated tools to help construct, verify proofs

- Things to bear in mind:
  - Can't use general-purpose theorem proving tools such as HOL, Coq, etc.
  - Tool should know how to do "reduction-based" proofs
  - Need to support well-known asusmptions, e.g., DLIN, SXDH, etc.
  - … And work with well-known notions of security, e.g., IND-CPA, IND-CCA1, IND-CCA2, EUF-CMA, etc.

CURRENT WORK IN CYBERSECURITY: Theory

- Tools exist for doing simple stuff, e.g.,
  - RSA proof of correctness
  - Reduction of crypto schemes to simple assumptions, e.g., Discrete Log, DDH
  - Some encryption schemes even proven IND-CPA secure
  - … But none for advanced cryptographic schemes such as attribute-based cryptosystems :-(

- Goal: Partially, or better, fully automate proofs of attribute-based encryption (ABE) (IEEE PST 2019, 2018)

- Challenges:
  - Mathematical assumpions *way* more involved than Discrete Log, factoring, etc.
  - Manual proofs very complicated, run into pages

FUNDING SOURCES

- Research funded by NSF award #1800088 (Aug. 2016 -- May 2020)
  - CRII: SaTC
  - PI: Vishwanathan

- New CREST Award: Center of Research Excellence in Design of Intelligent Technologies for Smart Grids
  - Senior Personnel for the security/privacy-related thrust of the project