Physical Unclonable Functions in IPv6 Deployment

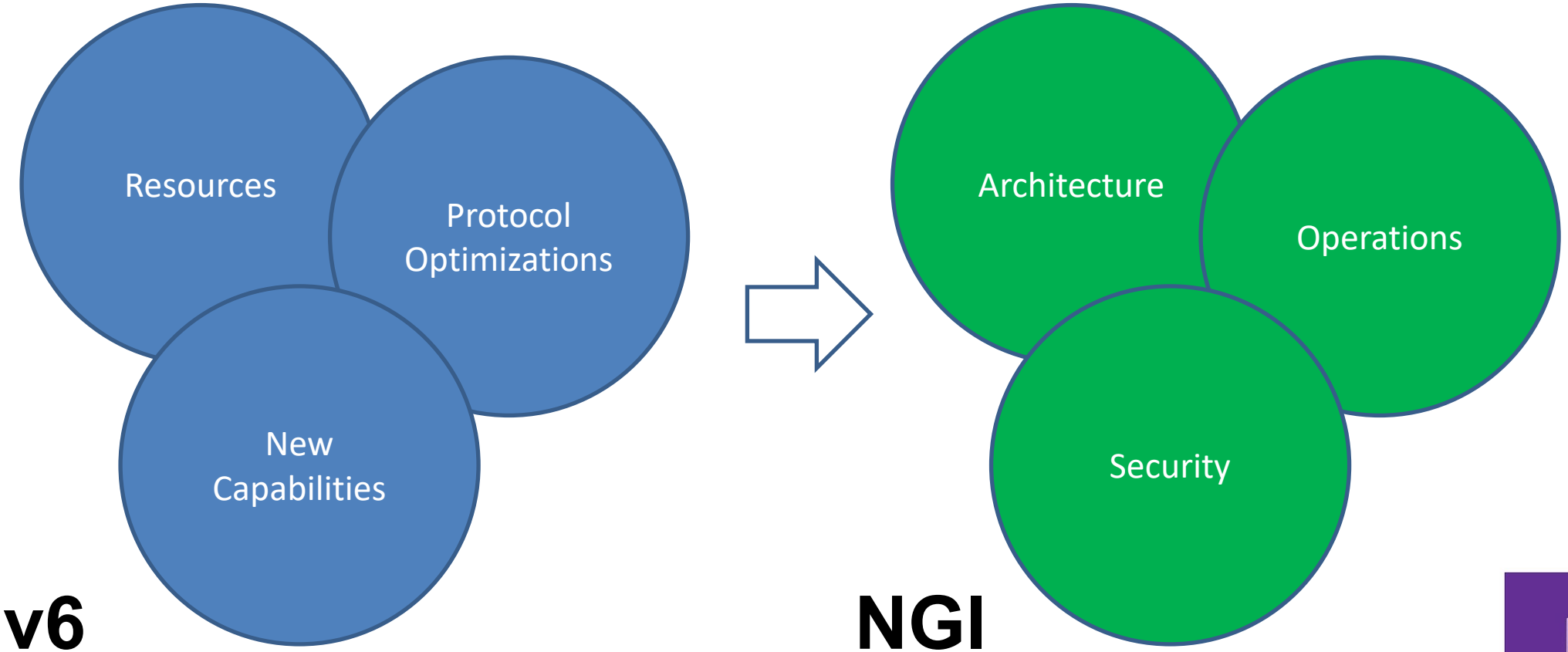
Ciprian Popoviciu
East Carolina University
Email: popoviciuc18@ecu.edu

www.isocore.com/2021

NET-CENTRIC

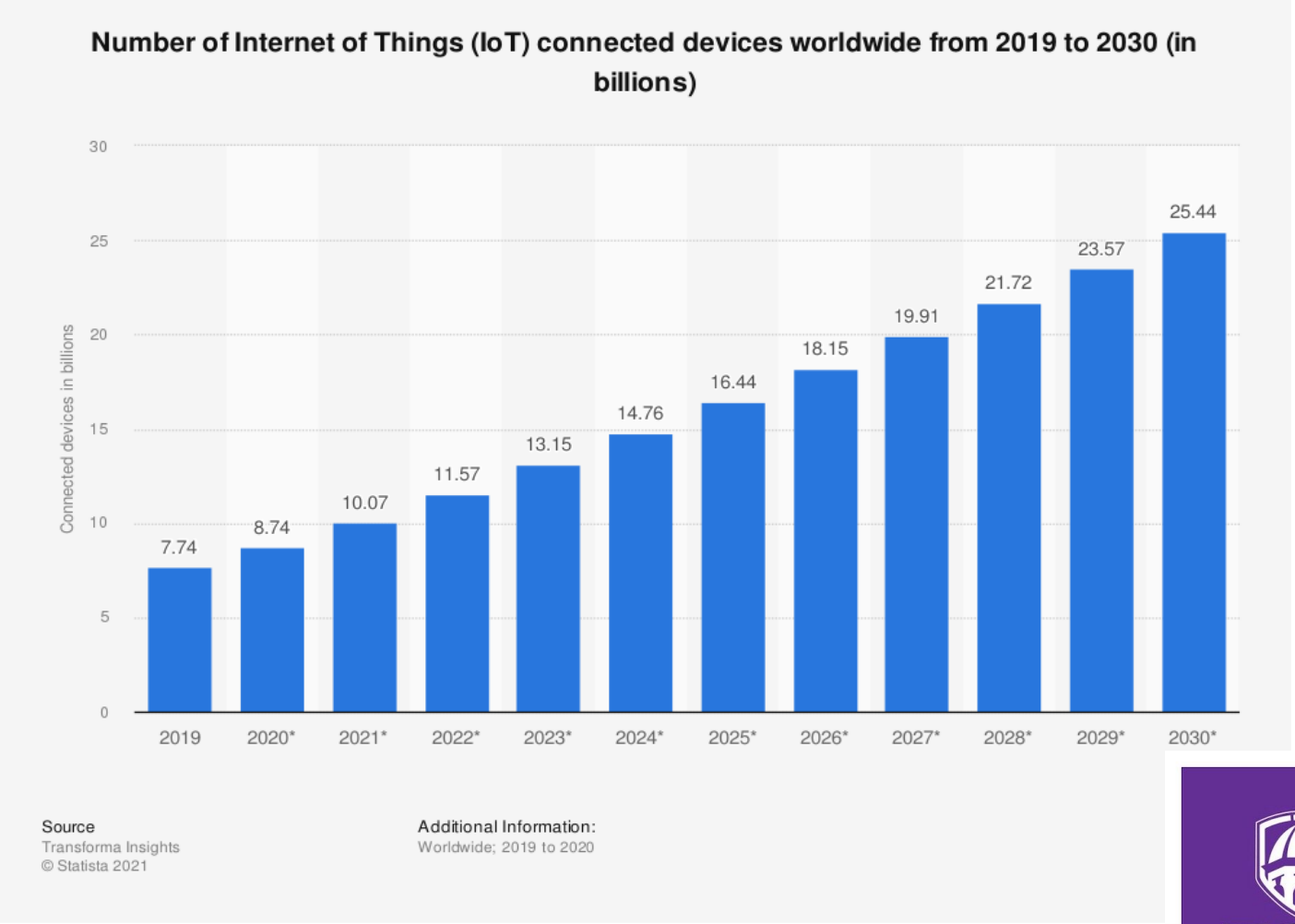
ECU

IPv6 and Next Generation Infrastructures



Accommodating Many Endpoints

- IPv6 Address Space
- Auto Provisioning
- NDP



NET-CENTRIC

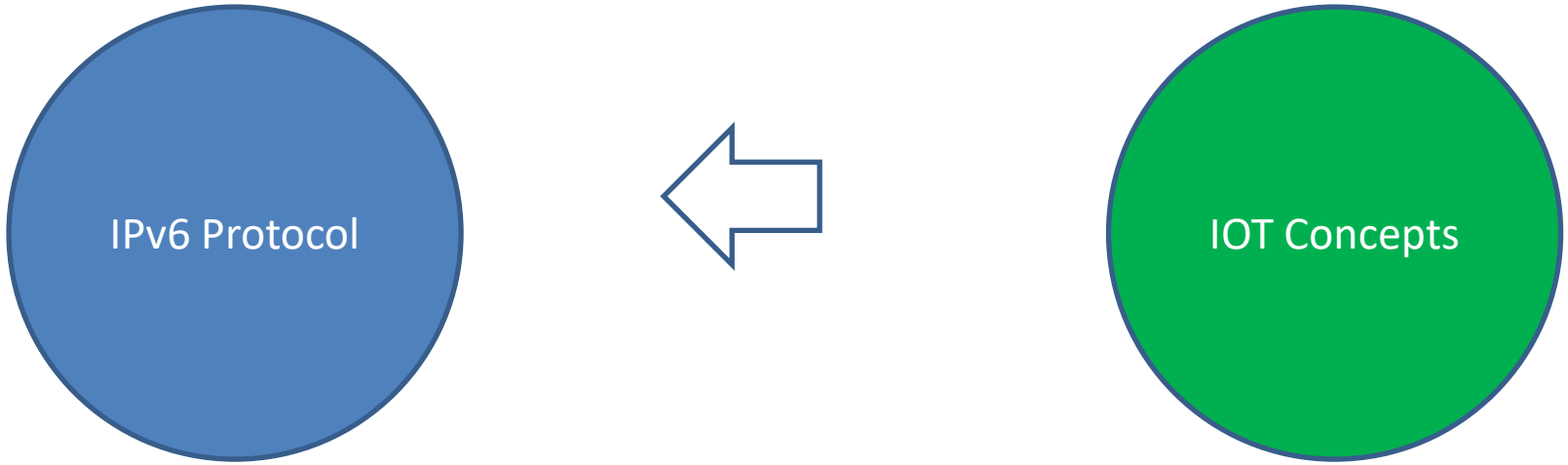
ECU

Securing Many Endpoints

- IPv6 Address Space
- CGA
- SEND

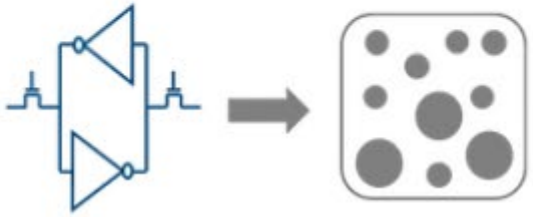
VS

- CPU/MEM Constraints
- Battery Constraints
- Bandwidth Constraints



Physical Unclonable Functions

Uncontrollable nano-scale process variations make ICs unique



Start–up SRAM values establish a unique Silicon fingerprint

Fingerprint turned into a strong secret cryptographic key

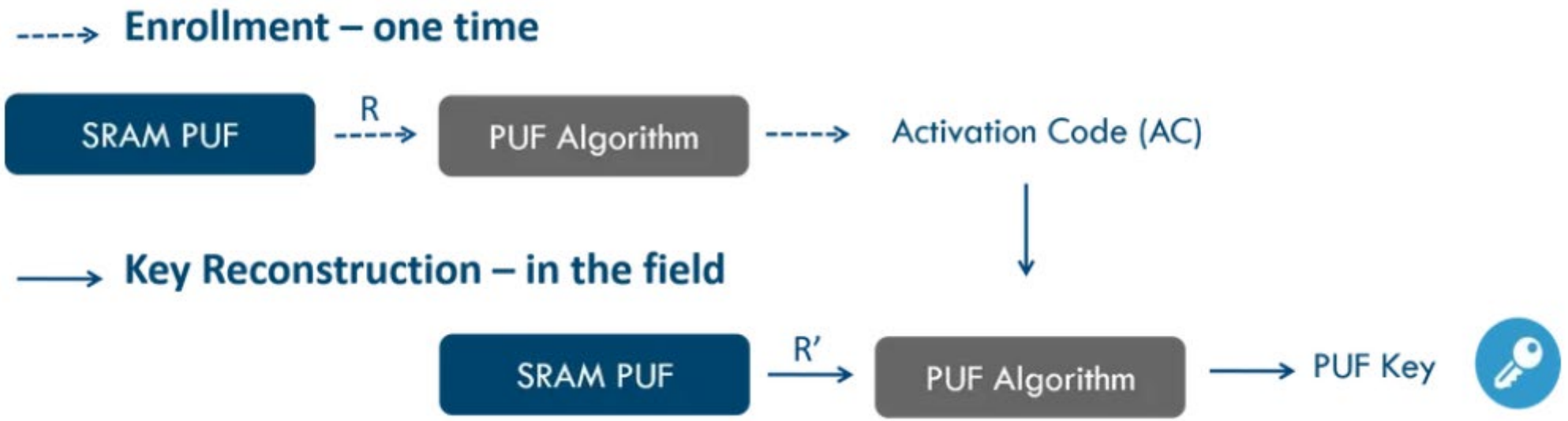
https://www.wevolver.com/article/sram.puf.the.secure.silicon.fingerprint

PUF is Efficient

E

https://www.wevolver.com/article/sram.puf.the.secure.silicon.fingerprint

PUF is Reliable



https://www.wevolver.com/article/sram.puf.the.secure.silicon.fingerprint

PUF & IPv6 – Protocol Considerations

- PUF + HMAC -> 64 bits IID -> CGA Alternative
- PUF + MAC + HMAC -> 64 bits IID -> Enhanced CGA Alternative
- Multiple PUFs -> Multiple Factor Authentication
- Less resources for encryption -> Light SEND

PUF & IPv6 – Operational Considerations

- Device registration and refresh processes
- PUF generation approach might require guidelines that ensure consistency
- To support scale, distributed authentication services might be needed

PUF & IPv6 – General Considerations

Benefits	Downsides
Less Demanding on Device Resources	Registration of Devices
More Secure (Resilient to firmware attacks)	New Authentication Services
More Implementation Options (availability)	Additional Integrations Across IT Services

PUF + IPv6 + NGI

- **IoT + Mobile** – With the rapid increase in mobile devices and IOT devices in the IT environment, operational support for PUF based authentication will become more common
- **Zero Trust** – With the adoption of Zero Trust, PUF based authentication is a natural element of a layered security architecture
- **Edge Computing** – With increased enablement of Edge Computing, authentication services can be distributed.

Conclusions

- IPv6 is the plan of record for IT infrastructures but it can evolve based on authentication techniques developed for specific use cases
- PUF is a mature technology providing an easy, reliable way to ID devices based on resources they already contain
- PUF offers an opportunity to optimize ND security and it can enable or benefit from other major NGI trends such as Zero Trust and Edge Computing

Thank You!

popoviciuc18@ecu.edu

NET-CENTRIC

ECU