University of Connecticut

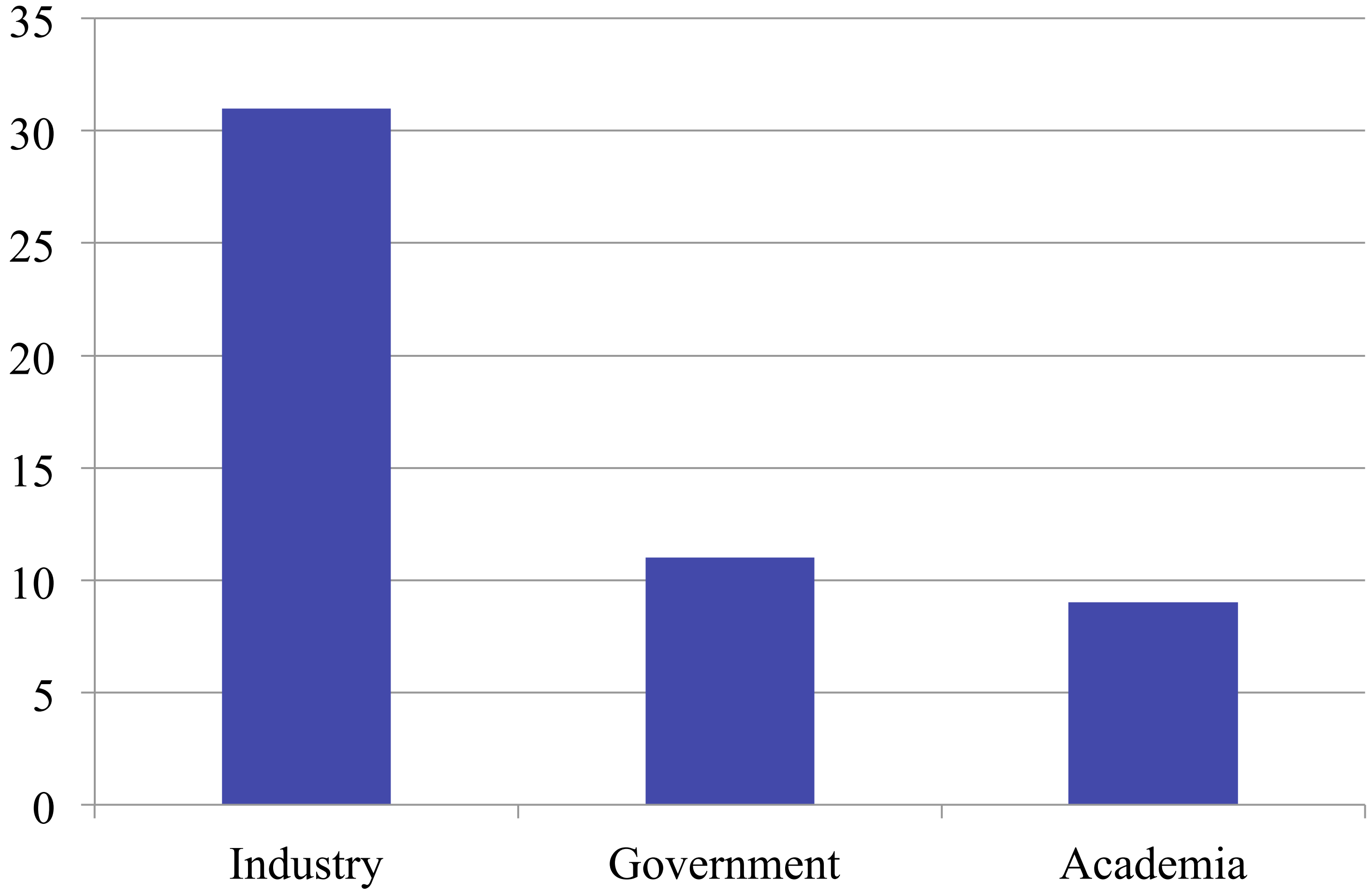
CHASE Survey on 6 Most Important Topics in Hardware Security

Prepared By Prof. M. Tehranipoor
Charles H. Knapp Associate Professor in Engineering Innovation

Topics

- Counterfeit Electronic Components and Supply Chain
- Hardware Security and Trust
- Reliability
- System Security
- Standards
- Emerging Threats

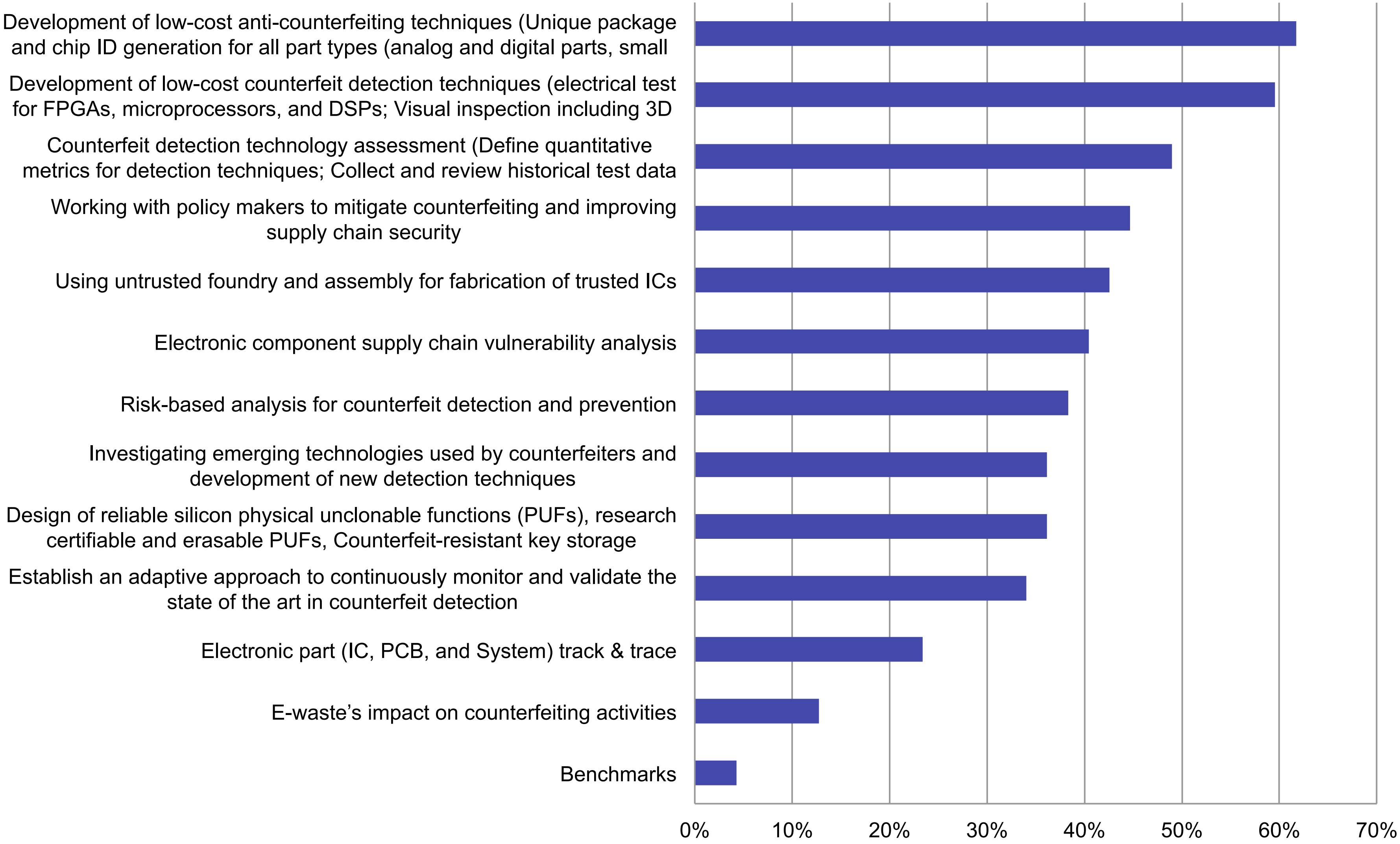
Distribution of Participants



Counterfeit Electronic Components and Supply Chain

Answer Choice	Responses in %	Responses in #
Development of low-cost anti-counterfeiting techniques (Unique package and chip ID generation for all part types (analog and digital parts, small and large ICs, passive and active components)	61.70%	29
Development of low-cost counterfeit detection techniques (electrical test for FPGAs, microprocessors, and DSPs; Visual inspection including 3D optical imaging, THz, etc. for all components; Margin tests (Flash, DRAM, SRAM, Microprocessors, etc.)	59.57%	28
Counterfeit detection technology assessment (Define quantitative metrics for detection techniques; Collect and review historical test data and evaluate effectiveness of test techniques, sequences and test combinations; Tools and methodologies for identifying a minimum set of tests to be performed for maximum test confidence; metrics to measure effectiveness of test techniques)	48.94%	23
Working with policy makers to mitigate counterfeiting and improving supply chain security	44.68%	21
Using untrusted foundry and assembly for fabrication of trusted ICs	42.55%	20
Electronic component supply chain vulnerability analysis	40.43%	19
Risk-based analysis for counterfeit detection and prevention	38.30%	18
Design of reliable silicon physical unclonable functions (PUFs), research certifiable and erasable PUFs, Counterfeit-resistant key storage	36.17%	17
Investigating emerging technologies used by counterfeiters and development of new detection techniques	36.17%	17
Establish an adaptive approach to continuously monitor and validate the state of the art in counterfeit detection	34.04%	16
Electronic part (IC, PCB, and System) track & trace	23.40%	11
E-waste's impact on counterfeiting activities	12.77%	6
Benchmarking	4.26%	2

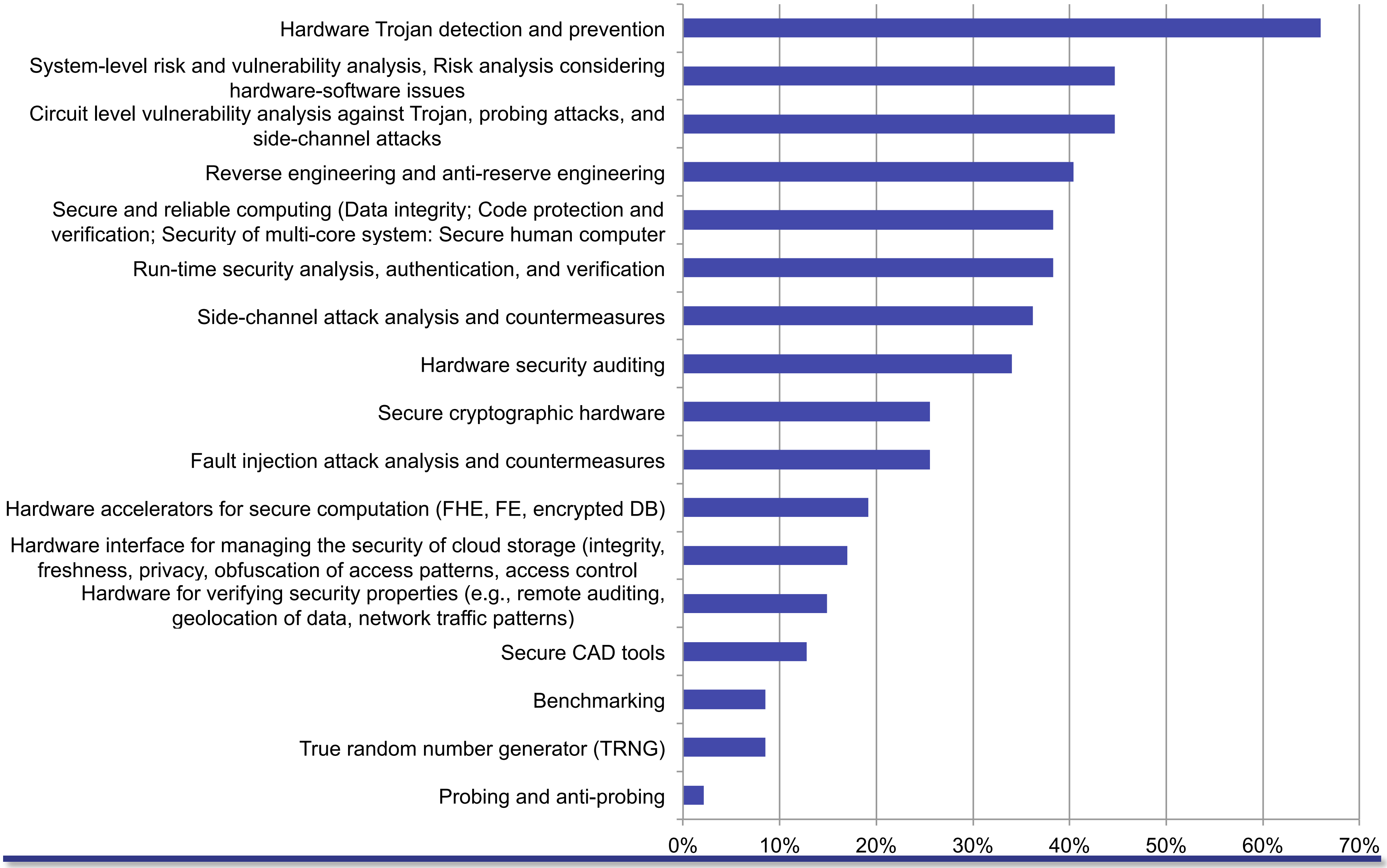
Counterfeit Electronic Components and Supply Chain



Hardware Security and Trust

Answer Choice	Responses in %	Responses in #
Hardware Trojan detection and prevention	65.96%	31
Circuit level vulnerability analysis against Trojan, probing attacks, and side-channel attacks	44.68%	21
System-level risk and vulnerability analysis, Risk analysis considering hardware-software issues	44.68%	21
Reverse engineering and anti-reserve engineering	40.43%	19
Run-time security analysis, authentication, and verification	38.30%	18
Secure and reliable computing (Data integrity; Code protection and verification; Security of multi-core system: Secure human computer interface)	38.30%	18
Side-channel attack analysis and countermeasures	36.17%	17
Hardware security auditing	34.04%	16
Fault injection attack analysis and countermeasures	25.53%	12
Secure cryptographic hardware	25.53%	12
Hardware accelerators for secure computation (FHE, FE, encrypted DB)	19.15%	9
Hardware interface for managing the security of cloud storage (integrity, freshness, privacy, obfuscation of access patterns, access control policy)	17.02%	8
Hardware for verifying security properties (e.g., remote auditing, geolocation of data, network traffic patterns)	14.89%	7
Secure CAD tools	12.77%	6
True random number generator (TRNG)	8.51%	4
Benchmarking	8.51%	4
Probing and anti-probing	2.13%	1

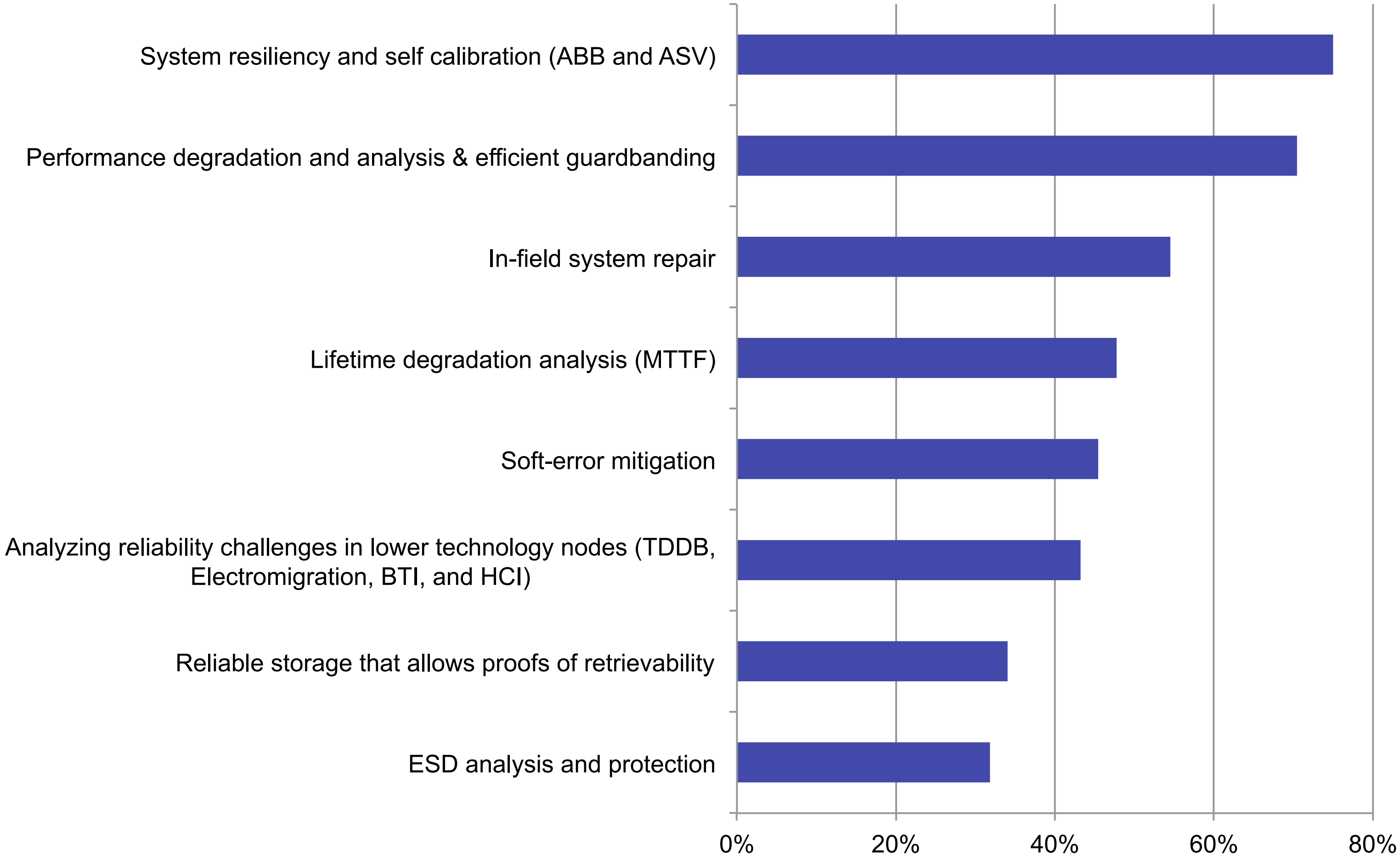
Hardware Security and Trust



Reliability

Answer Choice	Responses in %	Responses in #
System resiliency and self calibration (ABB and ASV)	75%	33
Performance degradation and analysis & efficient guardbanding	70.45%	31
In-field system repair	54.55%	24
Lifetime degradation analysis (MTTF)	47.73%	21
Soft-error mitigation	45.45%	20
Analyzing reliability challenges in lower technology nodes (TDDB, Electromigration, BTI, and HCI)	43.18%	19
Reliable storage that allows proofs of retrievability	34.09%	15
ESD analysis and protection	31.82%	14

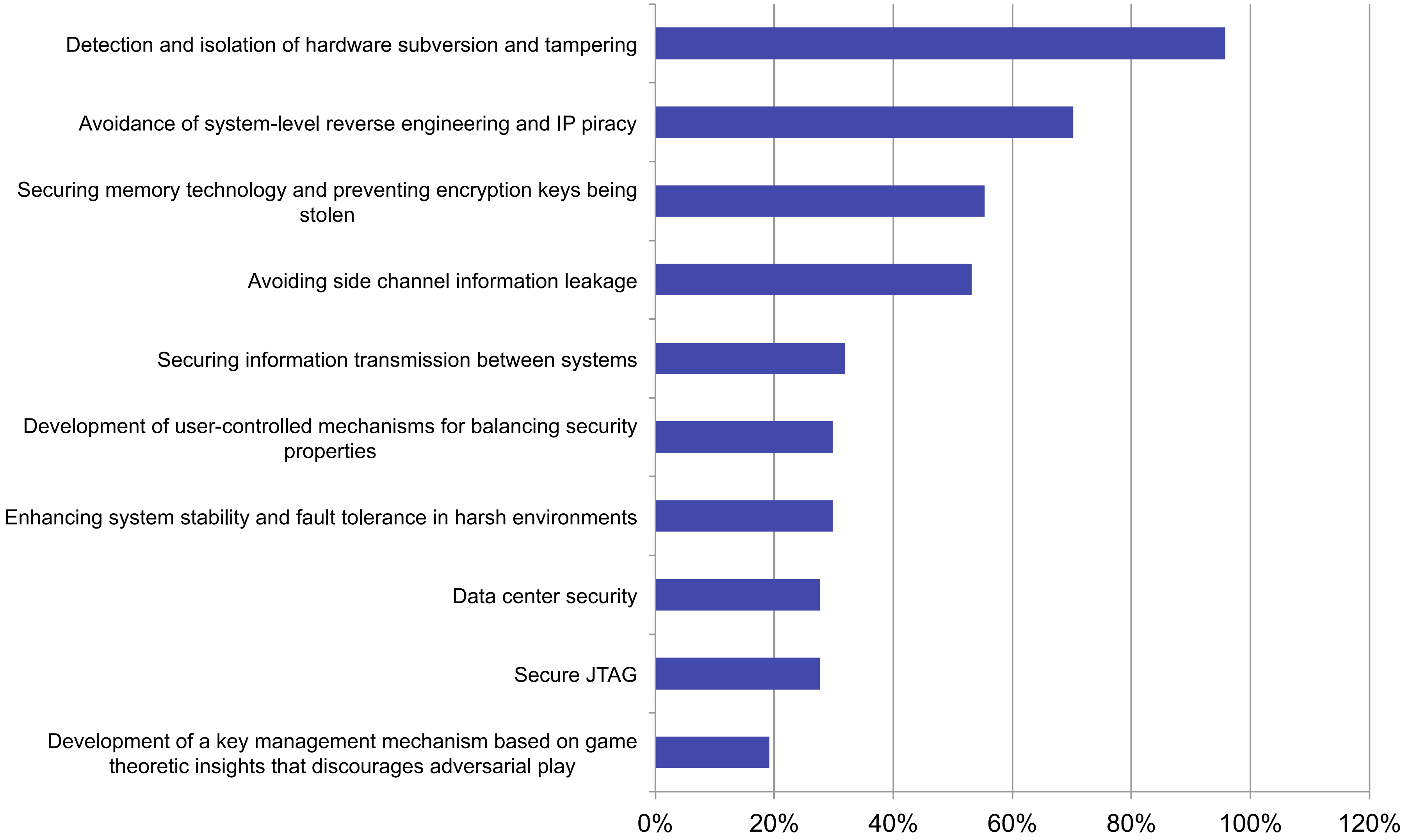
Reliability



System Security

Answer Choice	Responses in %	Responses in #
Detection and isolation of hardware subversion and tampering	95.74%	45
Avoidance of system-level reverse engineering and IP piracy	70.21%	33
Securing memory technology and preventing encryption keys being stolen	55.32%	26
Avoiding side channel information leakage	53.19%	25
Securing information transmission between systems	31.91%	15
Enhancing system stability and fault tolerance in harsh environments	29.79%	14
Development of user-controlled mechanisms for balancing security properties	29.79%	14
Secure JTAG	27.66%	13
Data center security	27.66%	13
Development of a key management mechanism based on game theoretic insights that discourages adversarial play	19.15%	9

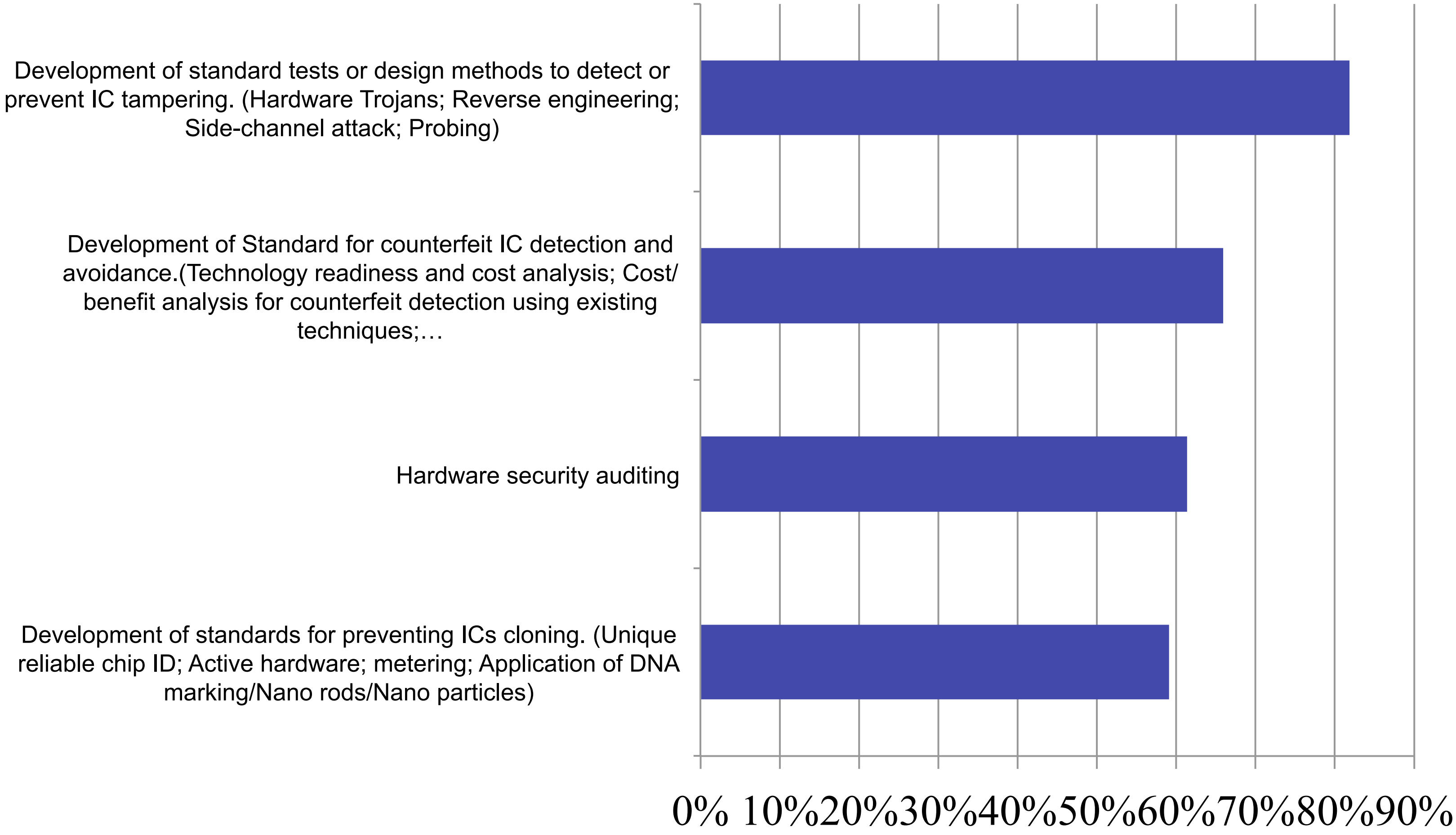
System Security



Standard Development

Answer Choice	Responses in %	Responses in #
Development of standard tests or design methods to detect or prevent IC tampering. (Hardware Trojans; Reverse engineering; Side-channel attack; Probing)	81.82%	36
Development of Standard for counterfeit IC detection and avoidance.(Technology readiness and cost analysis; Cost/benefit analysis for counterfeit detection using existing techniques;…	65.91%	29
Hardware security auditing	61.36%	27
Development of standards for preventing ICs cloning. (Unique reliable chip ID; Active hardware; metering; Application of DNA marking/Nano rods/Nano particles)	59.09%	26

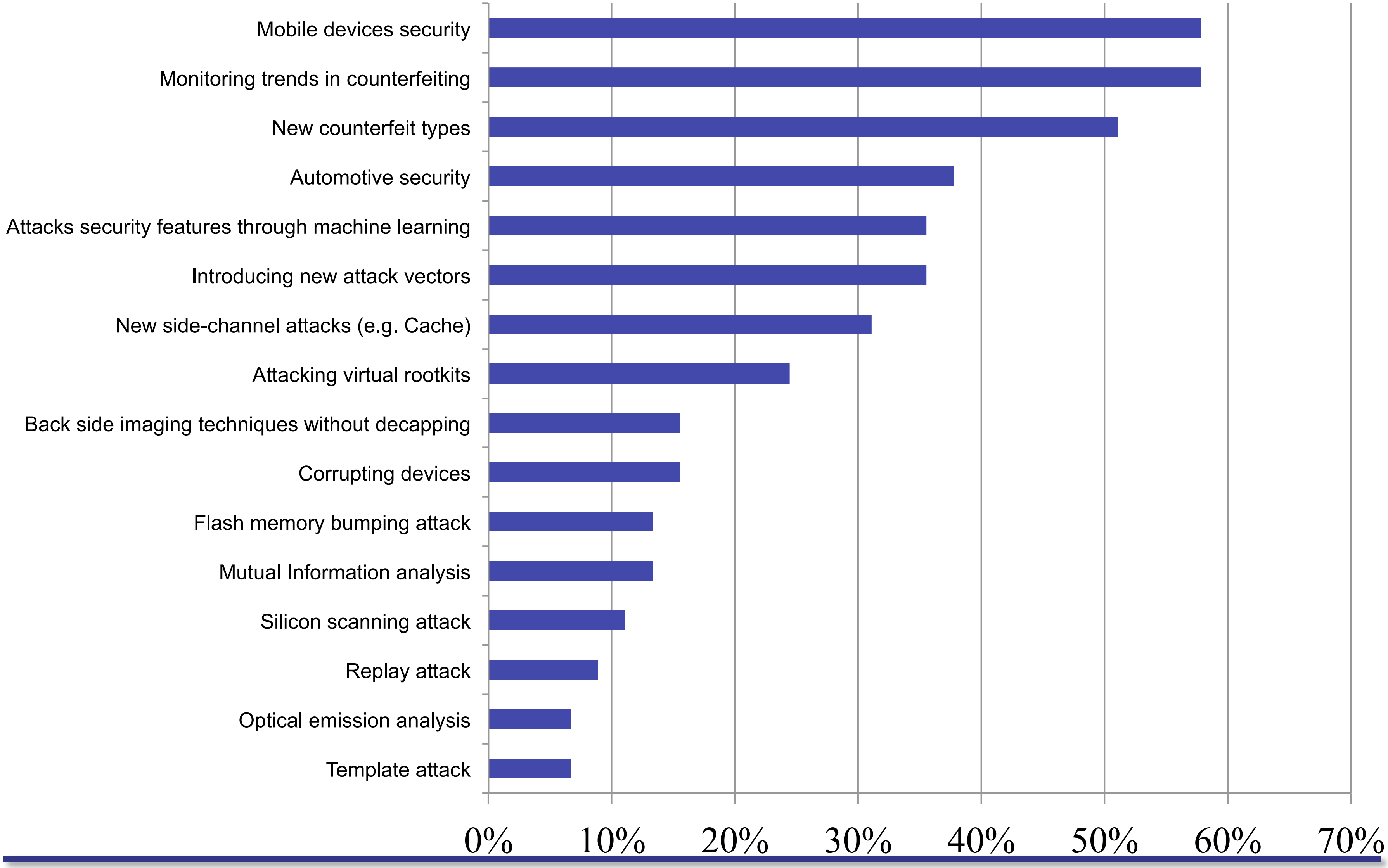
Standard Development



Emerging Threats

Answer Choice	Responses in %	Responses in #
Monitoring trends in counterfeiting	57.78%	26
Mobile devices security	57.78%	26
New counterfeit types	51.11%	23
Automotive security	37.78%	17
Introducing new attack vectors	35.56%	16
Attacks security features through machine learning	35.56%	16
New side-channel attacks (e.g. Cache)	31.11%	14
Attacking virtual rootkits	24.44%	11
Corrupting devices	15.56%	7
Back side imaging techniques without decapping	15.56%	7
Mutual Information analysis	13.33%	6
Flash memory bumping attack	13.33%	6
Silicon scanning attack	11.11%	5
Replay attack	8.89%	4
Template attack	6.67%	3
Optical emission analysis	6.67%	3

Emerging Threats


Mobile devices security
Monitoring trends in counterfeiting
New counterfeit types
Automotive security
Attacks security features through machine learning
Introducing new attack vectors
New side-channel attacks (e.g. Cache)
Attacking virtual rootkits
Back side imaging techniques without decapping
Corrupting devices
Flash memory bumping attack
Mutual Information analysis
Silicon scanning attack
Replay attack
Optical emission analysis
Template attack